TNO Information and Communication Technology

TUCK SCHOOL OF BUSINESS AT DARTMOUTH
Glassmeyer/McNamee
Center for
Digital Strategies

Brassersplein 2
P.O. Box 5050
2600 GB Delft
The Netherlands

www.tno.nl

T +31 15 285 70 00
F +31 15 285 70 57
info@telecom.tno.nl

TNO report

33680

International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues

Date	June 30, 2005	
Author(s)	Robert Bruce	Research Fellow, Center for Digital Strategies, Tuck School of Business
	Scott Dynes	Research Fellow, Center for Digital Strategies, Tuck School of Business
	Hans Brechbuhl	Executive Director, Center for Digital Strategies, Tuck School fo Business
	Bill Brown	Director Scenario Development, Institute for Security Technology Studies, Dartmouth College
	Eric Goetz	Research Associate, I3P, Dartmouth College
	Pascal Verhoest	TNO Information and Communication Technology, Delft, Netherlands
	Eric Luiijf	TNO Defence, Security and Safety, The Hague, Netherlands
	Sandra Helmus	TNO Information and Communication Technology, Delft, Netherlands

Number of pages	191
Number of appendices	2

All rights reserved.
No part of this publication may be reproduced and/or published by print, photoprint, microfilm or any other means without the previous written consent of TNO.

In case this report was drafted on instructions, the rights and obligations of contracting parties are subject to either the Standard Conditions for Research Instructions given to TNO, or the relevant agreement concluded between the contracting parties. Submitting the report for inspection to parties who have a direct interest is permitted.

© 2005 TNO

EXECUTIVE SUMMARY

Cyber security is a uniquely challenging policy issue with a wide range of public and private stakeholders within countries and beyond national boundaries. This executive summary and the full discussion paper delineate the need on a high priority basis to address cyber security issues and develop an effective and comprehensive national and international policy framework for protecting the information and communication technology (ICT)-based critical information infrastructures of nations. The paper is intended to focus international discussion, raise the sense of urgency attached to cyber security concerns, and provide impetus to new stakeholder initiatives.

1. Introduction

The rapid adoption in emerging countries of the new information and communication (ICT) infrastructures such as the internet is creating new opportunities for these countries and their citizens to participate in the world's flow of information, ideas and commerce. A good example of this is India, which in the past decade has gone from being a bit player to a major player in software development. The internet played a key role in enabling this transformation by collapsing geographic distances, allowing India's talent to compete on the same footing as programmers in the 'old' economies. This "flattening" of the world allows everyone to compete globally for information-based work. ICT Ministers have been seeking to stimulate the use of the internet and similar technologies to offer their citizens a broad range of improved services provided by government as well as the private sector. However, new opportunities offered by the use of ICT also generate new risks and vulnerabilities.

In developing countries, ICT Ministers are also seeking to stimulate the use of the internet and similar technologies to broadly offer their citizens new e-economy and e-government services such as email and online banking, often for the first time. These efforts may be vulnerable due to a lack of cyber security; there are reports that the great majority (95%) of email traffic in developing countries is spam. This level of spam discourages people from using email, greatly decreasing the utility of email, and reduces user's confidence in any online activity.

Multinational corporations who are seeking to do business in such countries, either by outsourcing tens of millions of dollars of work or investing hundreds of millions of dollars to build a plant locally, have to be certain that ICT-based capabilities they develop are going to be accessible and secure. This means that countries who want investment must have a rational approach to cyber security—it is becoming part of the package corporations must and will consider.

This discussion paper is intended to deal head-on with potential cyber security-related risk factors created by the increasing dependence of government and key sectors of the global economy on ICT and ICT-based services. The paper is fundamentally about providing Ministers of ICT and other interested entities a way of thinking about creating the right conditions to allow new e-economy and e-government services to contribute to significant economic growth and open, transparent, and vibrant societies. The paper provides guidance especially to government ministers with ICT portfolios and telecom regulators about the multi-dimensional aspects of cyber security policy concerns. This paper is also valuable for public officials concerned with economic policy and risk management, as well as with international and national security policy.

The ideas expressed in this summary are the key ideas of the paper briefly presented; we refer the reader to the discussion paper for a complete exposition.

2. Cyber Security: A Collective Concern

In a networked world, there are no real safe harbors—if you are on the network, you are available to everyone else on the network. A key consequence is that security is not the concern of someone else; of necessity it is the concern of everyone, a collective concern that must transcend national boundaries.

For example, major cyber security issues today include email spam and denial-of-service (DoS) attacks. The majority of spam and DoS attacks originate from BOT networks, networks of many thousands computers that are controlled by hackers. The main source of computers for these networks is in the homes of people who have always-on broadband connections to the internet, but who don’t have sufficient levels of cyber security measures taken. Through a virus or worm, the machine is ”recruited”—a program is loaded on the computer that allows remote control. The owner of the computer often does not even notice the recruitment of their computer. Here, a major source of internet pain is the direct result of home users not taking care to protect their machines. The spread of such recruitments can turn poorly protected parts of national networks—whether residential users or university-based computer processing centers—as well as entire national networks with inadequate security—into staging areas for potential attacks on critical information infrastructure within a country or beyond its borders. Similar vulnerability concerns exist in the corporate sector and elsewhere as a result of information system interdependences.

Because the internet has no natural political boundaries, national boundaries are not effective to partition cyber security policy responsibilities. And even though security is a basic public sector concern, and typically regulated at the government level, the bulk of the capability for dealing with cyber security risk is not in the hands of governments but lies with the private or semi-private sector entities that actually manage and operate the ICT infrastructure.

This is why cyber security is such a complex and novel area of public policy concern. It is also why this discussion paper is necessarily ambitious in scope and deals with issues that are very difficult to put into easy, airtight compartments. Cyber security concerns cannot be dealt with easily by market forces or by regulation but require a novel mix of solutions. These concerns are not the exclusive domain of economists, political scientists, lawyers, business policy or management experts, or computer specialists—or even of national security experts or telecom regulators. Rather, a highly diverse group of stakeholders or key actors—working in their own domains and in concert—has a potential role in orchestrating the set of functions (described fully in the document) that in aggregate result in an effective cyber security policy.

Each stakeholder will need to take actions or communicate with other key actors in the private sector, semi-private sector, or the government, nationally or internationally. As a result, any effective approach to cyber security will result in a complex network of conversations among public and private entities both in a national and international context. These communications are seamless, having no bounds or limits—geographical or jurisdictional.

A Network of Conversations

Cyber security is essentially about managing future risk and responding to current and past incidents and attacks. Managing future risk requires insight into current and future vulnerabilities and how to prevent or reduce them, the probabilities of a threat, and the costs associated with potential outcomes and how to mitigate them. Responding to current and past incidents and attacks requires knowledge of what has happened, methods of preventing similar incidents from being successful in the future, and possible legal or other remedial actions against the perpetrators.

A key point is that these risk management approaches have basically similar elements whether you are looking at a small company, a very big multinational corporation, or a nation. Another key point is that many of these essential activities require communications across “organizational” boundaries, be they firm, national or other. To know the probabilities of a certain threat, one needs to talk to stakeholders in other entities and at different levels. To be aware of threats that others have encountered and handled, there has to be a constant flow of information. Legal or other remedial action may often also require international cooperation.

To bring clarity to these ideas, we have adopted a network model of the interactions that are needed for effective cyber security. This network model (see Figure 1) consists of nodes that collaborate in the performance of various key elements or functions of a cyber security framework. Examples of nodes include various governmental bodies such as ministries, private or semi-private agencies including computer emergency response teams (CERTs), information sharing and analysis centers (ISACs), vendors, service providers, firms, etc. These nodes exchange information related to functional areas involved in a cyber security framework. The content of these Information Flows depends on the function-specific responsibilities of the communicating nodes. Examples of functions include threat assessment and incident response. These nodes function via the sharing of information with other nodes associated with the function. The collaboration between nodes gives rise to Obligations and Expectations between stakeholders in the nodes. These relationships can be structured by contract, formal or informal agreements, or administrative procedures or requirements. These relationships can be used as a mechanism for imposing responsibilities or holding counterparts accountable for the activities of networked relationships that are within the span of control of the parties to a paired relationship.

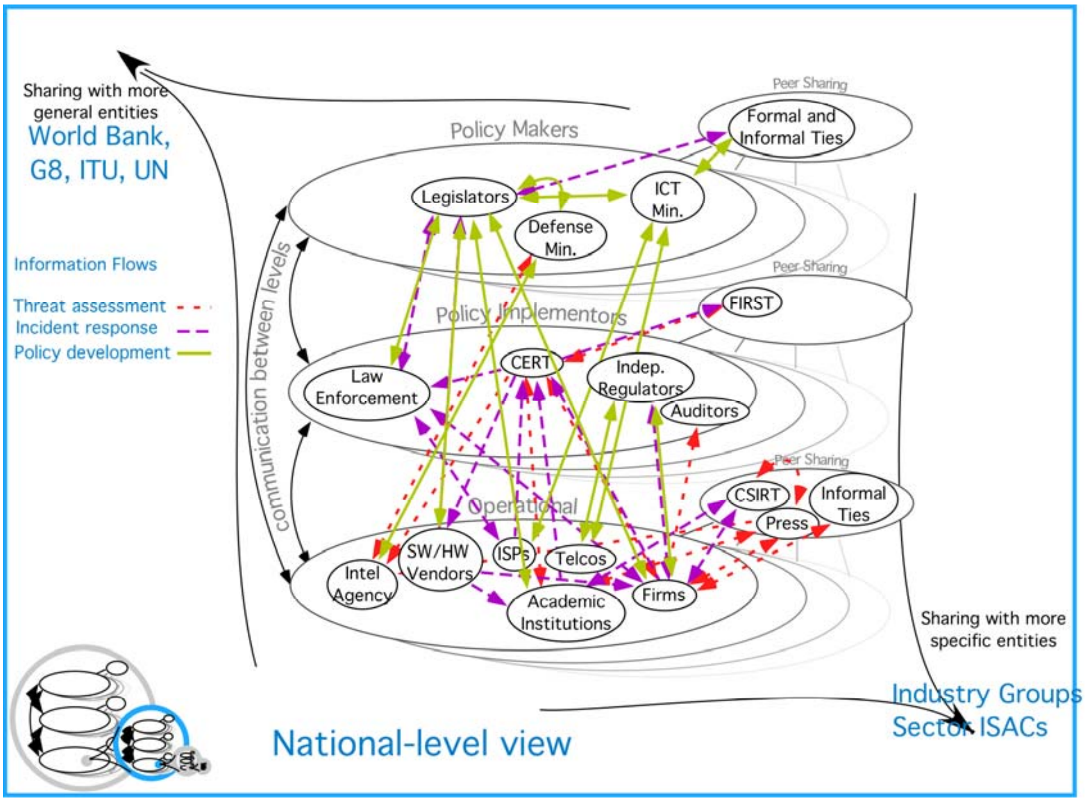


Figure 1: Example of Nodes and Information Flows at a National Level. For three functions (shown at the left) a possible set of nodes and flows of information between those nodes is shown. Nodes representing "peer sharing" represent formal ways for nodes to share information with their peers; it has been shown that informal communication channels are also very important, particularly during emergencies. Notional diagrams such as this can serve as assessment tools: a communication flow present in the diagram but not in real life is an opportunity for improvement.

This "network-oriented approach" to cyber policy has the advantage of encouraging all stakeholders to act on the basis of a shared vision of the challenges and required responses. Telecom regulators, ICT- and other public officials should promote this shared vision both internally, within their public and private sectors, as well as internationally. Another advantage is promoting thinking in terms of functions, rather than titles or national or international institutions. A key recommendation is the development of collaborative relationships among countries in the area of cyber security that are focused on the coordination of key functions as well as the meshing of key processes and procedures necessary in each country to deal with the key functions a cyber security framework. As countries are likely to have different titles or institutions for dealing with the same roles and responsibilities, mapping their institutions and titles to the roles in the network model will be very helpful in assuring that different national cyber security structures can inter-operate effectively.

These ideas are illustrated in the accompanying figures (see Figure 1 above and Figure 2 below)

National Policy Implications

The discussion paper lays out a complete set of national policy recommendations; here we summarize only the key national policy themes.

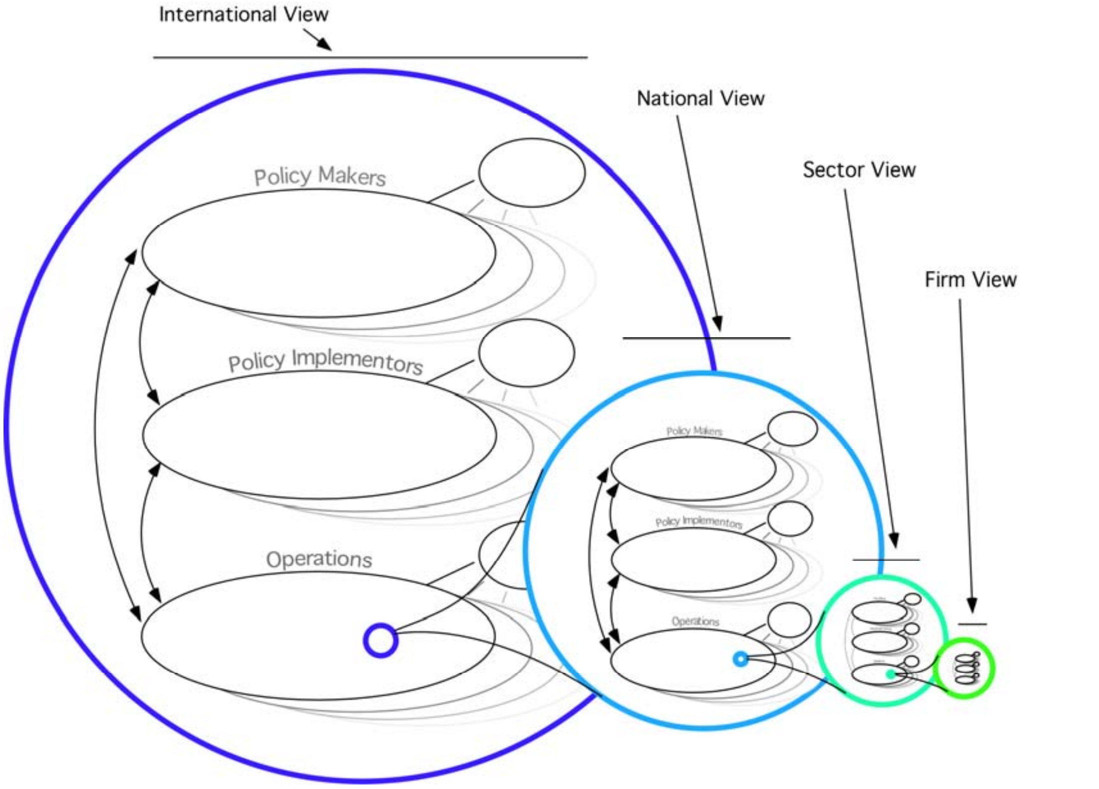


Figure 2: The Fractal Nature of Information Flows. As noted in the text, the nodes and information flows will be very similar within different entities regardless of their size as the same functions need to be carried out at each level. This figure should make clear that cyber security is a collective effort, and that every entity has responsibilities to every other entity

Raising Awareness of Cyber Security in Your Environment

As we hope will be clear even from this brief overview, cyber security is not something “done” by one person, but is a shared responsibility among all connected with and who use the ICT infrastructure. It follows that one key element of effective cyber security policy must be creating the right awareness of and incentives for cyber risk management at all levels: home computer users, small and large corporations (who likely are the main components of the critical infrastructure), as well as local and national governments. This should take the form of comprehensive educational initiatives including promoting the enculturation of cyber security best practices in technical practices, promoting risk management practices in business settings. These efforts go hand-in-hand with developing the necessary flows of information described above.

Perhaps most important educational efforts are “public health” type educational initiatives (e.g. “safe surfing”) for increasing awareness of the importance of cyber security in the general public. One key aim is creating market expectations, particularly at the level of the general public, that cyber security need to be integral to products and services and must be designed and built in from the start, not bolted on as an afterthought.

As awareness increases there will be a demand for information about the risk so users can make informed decisions regarding cyber security. Potential threats are not easy to assess. They are constantly changing and are technologically driven, evolving as new capabilities are introduced, and as the ICT infrastructure becomes more complex with the addition of new network architectures such as wireless and mobile features. The full dimensions of cyber incidents will require the sharing of information between private firms, suppliers of products and services, and from public agencies including intelligence and security agencies.

While regulatory agencies or ICT ministries have not generally been central players in dealing with cyber security, they can play a crucial role along with their private sector counterparts such as international and national chambers of commerce in enabling others to assess their risk. They can highlight best practices for providers of telecom and internet-related infrastructure, and track and monitor emerging technological developments from a cyber risk perspective. They can help increase awareness of cyber risks by users of telecom and internet-related services. A government as a whole can enact policies that promote or inhibit information sharing regarding cyber security. Some examples include creating entities such as computer emergency response teams and creating rational policies relating to information disclosure or dissemination.

As important as raising awareness is, the goal is promoting action resulting in an appropriate level of cyber security. Some possible policy mechanisms include strengthening market signals or pressures to enhance levels of cyber security or "targeting" information flows (in the case of risk-related information through which the performance of "networks" dealing with cyber may be influenced), strengthening the influence of market-related drivers through government procurement policies, allocating liability among service providers and users, or imposing regulatory requirements relating to cyber security.

Becoming a Good Cybercitizen in the International Environment

Because the internet has no boundaries, everyone is affected by the cyber security choices of others. As noted in the recruited computers example above, most of the email spam is generated by home user machines that are poorly protected; they are an example of a "weak link" that potentially causes a break-down of the whole ICT infrastructure.

Much important and innovative work has been done to identify the key "principles" for cyber security policy—for establishing what the OECD has described as a culture of security. The OECD Guidelines for the Security of Information Systems and Networks and subsequent work on the implementation of these guidelines by OECD countries is a very important reference point for establishing baseline cyber security policies among countries around the world. Likewise, case studies and the careful empirical documentation of cyber frameworks in a number of key industrialized countries are another pillar and key underpinning for future policy initiatives.[1]

There are obvious risks to allowing weak links to develop in global networks which can create significant vulnerabilities within an inadequately protected country and/or for all countries. Policy makers should focus attention on adopting minimum requirements for ensuring cyber security so that they are not a weak link.

Developing International Relationships

Effective cyber security policy requires a wide range of international collaborative activities. This needs to take place at different levels between governments—and between private sector stakeholders. These contacts must be both bilateral and multi-lateral.

The reasons for these international collaborations include information sharing on risks, vulnerabilities and best practices, developing formal and informal working relationships with key stakeholders in other countries with comparable roles and responsibilities, and enabling the assessment of one's efforts against those of similar countries. Many developing countries have yet to become part of the international dialogue about cyber security. The circle of international dialogue needs to be widened; new consultative venues and resources may be required to do this.

Another reason is improving the inter-operability of cyber security policy frameworks—the set of processes and procedures through which different national frameworks can interact with each other. Inter-operability implies that stakeholders in each national cyber scheme understand how to communicate with each other to carry out key elements of a cross-border framework; this is a critical policy concern since it is likely that

[1] The 2004 CIIP Handbook and other relevant reference materials prepared by the Swiss Federal Institute of Technology can be found at www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224. These materials provide extraordinarily useful country case studies and other materials on differing approaches to risk management undertaken by national, regional, and international organizations.

the environmental and structural factors specific to each country result in substantially different architectures and performance of national networks.

International Policy Implications

The international community should commit to developing the necessary resources and capabilities to implementing more effective cyber security policies on an international basis. Many multinational organizations including the ITU, the IETF, the World Bank, the OECD, and the European Union, have a role in dealing with some, but not all, aspects of such initiatives in connection with the World Summit on the Information Society .

There is a need to promote the development of information flows between countries through collaborative research and information gathering. The scope of such an undertaking is described more fully in the discussion paper. The collaborative undertaking should involve building a critical mass of institutions concerned with cyber security policy both in developed and developing countries. It should involve both continued collection of institutional case study-related information as well as more focus on the economic and other drivers behind the “network model” described in this discussion paper. We hope that this discussion paper—the network model described therein—as well as the collection of background documentation included on a related wiki site—can be further refined, evaluated, and updated through a broader scale international undertaking.

We believe that it is critically important that discussions about cyber security policies reach out to a wider circle of countries than is currently involved in various bilateral, regional, and international consultations on cyber security policy. The Global Regulatory Exchange of the International Telecommunications Union may be one useful channel to utilize in broadening the current international dialogue about cyber security policy among telecom regulators and ICT ministers if they enlarge their constituency with and embrace the wider internet community. We also believe that cyber security may be a good subject for a series of virtual roundtables that might be organized through the Global Distant Learning Network of the World Bank.

Policy makers can usefully focus on a “node-to-node” approach to improving flows of information and collaborative relationships between national policy makers and international counterparts such as among CERTs or among firms or industry associations operating on a cross-border basis. One mechanism we are recommending is to develop these functional relationships are cyber exercises among a group of countries. These cyber exercises could perhaps be modeled after the “TOPOFF” exercises in the U.S. or be a series of more basic “table top” exercises. These exercises could provide an impetus for countries to map their cyber security processes against the network model as part of interfacing with other countries’ cyber security processes.

The development of new communication channels among countries would achieve the objective of improving international collaboration and bringing additional countries into the international dialogue about cyber security. Additionally, such exercises would serve as an assessment tool, both from the viewpoint of the exercise itself as well as from the standpoint of creating norms and benchmarks. We believe a most useful activity would be for an international nongovernmental entity (possibly the international research consortium mentioned above) to develop a “cyber-exercise-in-a-box” and maintain a staff whose purpose would be to recruit countries and run such exercises.

3. Conclusion

This discussion paper offers a detailed look at international and national policy issues surrounding cyber security. Cyber security is a uniquely challenging policy issue with a wide range of public and private stakeholders within countries and beyond national boundaries. The required approach of shared responsibility in both a national and international context—among public and private sector entities—makes normal governmental policy mechanisms only partially effective at best.

In the discussion paper, we discuss, more fully than we have in this brief summary, a network approach that makes clear the interdependencies and mutual responsibilities, and points out the need for collaborative actions. We make various recommendations aimed at enabling government and international entities to create the right conditions to allow new e-economy and e-government services to contribute to significant economic growth and open, transparent, and vibrant societies.

Table of Contents

Page

Executive Summary i

1. Introduction... i
2. Cyber Security: A Collective Concern ii
3. Conclusion vii

I Introduction: Overview of Key Issues Confronting International Policy-Makers...4

1. Pace of Technological Changes: Revolutionary Impact of IP-Technology.................. 9
2. Dealing with the "Dark Side" of E-Opportunities 11
3. Sources of New Threats: Blend of Hackers, Cyber Criminals, Terrorists, and High-tech National Security Strategists:.. 13
4. Nature of New Threats: From Denial of Service to Attacks on Data Authenticity... 14
5. "Weak Links" in the Global Information Infrastructure:... 15
6. Key Questions Facing Cyber Policy-makers 17
7. Basic Rationale for Focusing on Cyber Security: Encouraging More Stable Climate for Investment and National Security Concerns 19
8. Complexity of the Challenge of Achieving Adequate Cyber Security: Both Regulatory and Market Forces May be Ineffective 18
9. Key Elements of a Cyber Security Policy Framework: A Network of Many Nodes and Information Flows.. 20

II Overview of Key Elements of an International Cyber Security Framework 24

1. Prevention of debilitating damage and minimization of the risk of cyber attacks 25
2. Assessment of potential range of threats 27
3. Assessment of vulnerabilities of critical information infrastructure........................... 32
4. Improvement of risk management in the public, semi-public, and private sectors 38
5. Improvement of information sharing on a formal and informal basis 53
6. Development of mechanisms to respond to cyber incidents...................................... 55
7. Improvement of regulatory tools and mechanisms for minimizing risk to telecommunications including the Internet-related infrastructure 58

Page

8. Devising effective law enforcement tools in response to cyber incidents or attacks ... 64

9. Development of security doctrine relating to sanctions and response to cyber attacks ... 68

10. Coordination, Command and Control, and Communication in Managing Cyber Security Policies ... 70

11. Improved quality of system and application software ... 72

12. Building New International Lines of Cooperation and Collaboration ... 74

III A Different Angle of Vision on the Cyber Security "Network Model": Key Nodes and Information Flows ... 77

1. Coordination among Public Sector Entities Concerned with Cyber Security ... 82

2. Central Coordination Entities: Managing "Outreach" and the Labyrinth of Information Flows ... 83

3. Independent Telecom Regulators and IT/ICT Ministers ... 89

4. Critical Information Infrastructure Agencies ... 103

5. Intelligence and National Security Agencies: ... 105

6. Law Enforcement Agencies ... 108

7. Computer Emergency Response Teams (CERTs) and ISACs ... 111

8. Coordination Among Entities in the Private Sector ... 113

IV Approaches to Improving Collaborative Networks for Dealing with Cyber Security ... 117

1. International R&D Coordination Networks ... 119

2. International Collaboration Networks ... 119

3. Exercises ... 120

V Key Policy Options and Recommendations ... 128

A Strengthening the International Framework for Dealing with Cyber Security Concerns ... 128

B Some Key Recommended Perspectives for Viewing Cyber Security Policy from the Standpoint of ICT and Other Officials Concerning with Cyber Security Policy ... 133

C Initiatives to Develop Enabling Resources for the Development of the International Cyber Security Policy Framework ... 149

Appendix A Case Study of a U.S. multinational firm and selected suppliers ... 154
Appendix B Further Information on CERTs and CSIRTs ... 179

Table of Contents

Page

GLOSSARY 188
REFERENCES 191

International Policy Framework for Protecting Critical Information Infrastructure: A Discussion Paper Outlining Key Policy Issues

II Introduction: Overview of Key Issues Confronting International Policy-Makers

Policy-makers and business executives around the world commonly acknowledge the growing importance of information and communications technologies (ICT). These technologies are reshaping, in a myriad of ways, services provided by businesses, organizations, and governments. However, an important dialogue is only just beginning to take shape concerning the potential downsides, societal risk factors, and far-reaching challenges of these revolutionary changes.

This discussion paper is intended to document emerging risk factors and challenges and stimulate discussions by policy-makers in the public, semi-public, and private sectors. It focuses, in particular, on the cyber risk to critical infrastructures. These infrastructures are generally accepted to be those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.[2]

Though the paper focuses on cyber risks, threats to critical information infrastructure, and a “black economy” growing in tandem with new IT-driven opportunities in the public and private sectors, it deals fundamentally with opportunity--opportunities for business innovation and societal development in critical areas of human

[2] Critical infrastructures are defined by the European Union, Critical Infrastructure Protection in the Fight against Terrorism, COM(2004) 702 Final, Communication from the Commission to the Council and the European Parliament..

concern. This paper outlines policies for dealing head-on with potentially grave risks created by the rapid infusion of ICT technology into the global economy. It is based on the view that such risks should not become a deterrent to new investment and rapid deployment of IT services. A cyber security policy framework should be viewed a critical part of an enabling framework for new e-economy opportunities.

A well-balanced cyber security policy framework is highly complex. Such a policy framework has no bounds or limits—geographical or jurisdictional. It necessarily encompasses a full spectrum of business, societal, and governmental interests. Though inevitably cyber policy addresses grave concerns about national and global security and well-organized and destructive criminal activity, it is fundamentally about creating the very underpinning for stable and significant economic growth and for open, transparent, just, and vibrant societies.

This paper assesses, in particular, the complex web of inter-relationships through which businesses, governments, and other societal organizations deal with concerns about cyber security. It describes those inter-relationships in terms of a “network model” that highlights the importance of the “lines of communications” that develop among key stakeholders in order to meet the challenges of protecting critical information infrastructure. It addresses, in particular, the ways in which governments, business, and other organizations deal with different dimensions of cyber security concerns—with the strategic, tactical, and operational aspects of an important and emerging area of public policy.

Governments have a critical role at the strategic level in providing a clear vision of potential risks and responses as well as leadership and political support in mobilizing required resources both domestically and internationally. Governments have open to them a spectrum of differing approaches including enacting new legislation or regulations, subsidizing critical security initiatives, mobilizing public awareness, or encouraging public-private partnerships to provide increased levels of information security[3] for critical information infrastructure services.

In implementing overall strategy, government officials including independent regulators, together with leaders of business and other organizations, must devise specific, nearer-term initiatives that establish what could be broadly described as the governance arrangements that will determine how critical infrastructure is protected through cooperation and collaboration among a range of public, semi-public, and private sector concerned stakeholders. These arrangements may result in a myriad of different mechanisms at an operational level through which security-related information is shared within individual firms and government agencies in order to protect against cyber risks critical information infrastructure-related services. These services include a myriad of different economic activities provided in industry sectors such as the financial services, telecom, public utility, or health-related sectors and other sectors significantly dependent on core sectors such as the telecom and electric power sectors.

In Part II of this discussion paper, we describe some of the key elements or functions of a cyber security framework. In Part III we look at these key elements of a cyber security framework from a different angle of vision. We view a cyber security framework as a complex multi-dimensional network of nodes and information flows. We believe that viewing cyber security arrangements as such a network can be an important tool for structuring and improving the management of potential risks. Often policy makers focus on institutions and functions when it can be actually helpful to look behind these institutions and functions at “processes” and “procedures”. These procedures and processes may sometimes be structured through government directives or practices or through formal or informal contracts. They involve expectations, obligations, and flows

[3] In this report we will use the term “Cyber security” as a notion to cover organizational, technical, and procedural aspects of information security related to information and communications technology.

of information—all of which of cumulatively and diversely in different national and institutional settings influence and shape how cyber risks are addressed.

This paper does not describe in definitive terms either how these systems actually operate or how they should operate. We do not know enough about these complex systems—how they behave, what impedes or facilitates them. Rather, it is intended to establish a framework for better understanding the dynamics of these "networks"—how they do or might operate in a national and an international context.

Much important and innovative work has been done in identifying the key "principles" for cyber security policy—for establishing what the OECD has described as a culture of security. The OECD Guidelines for the Security of Information Systems and Networks and subsequent work on the implementation of these guidelines by OECD countries is a very important benchmark and reference point for establishing future cyber security policies among an ever widening circle of countries around the world.

Likewise, the case studies and the careful empirical documentation of cyber frameworks in a number of key industrialized countries is another pillar and key underpinning for future policy initiatives. We believe that it is critical to focus on how "principles" can be put into practice through procedures and practices and how policy frameworks actually work rather than on institutional mandates and jurisdictions.

Part III thus details various institutional nodes or platforms including so-called information sharing and analysis centers (ISACs) as well as institutions known as Computer Emergency Response Teams (CERTs) set up to respond to threats and cyber-related incidents and emergencies with potential differing scope and impact[4].

[4] See Section III6 for further discussion of the role of CERTs and ISACs.

What is clear is that there is no single strategy, set of governance arrangements, or operational practices that are right for every country. There are, of course, differences in legal systems, economic development, and trust between the government and the private sectors due to different cultural and historical backgrounds. However, it is also undeniably important to develop within, and among, countries improved lines of communication based on relationships of trust that evolve recognizing differences in background and national experience.

This paper is focused, in particular, on how differing schemes or national networks can be made to be more “inter-operable”. It is intended to highlight a “minimum” or core set of capabilities that are an essential condition for being an integral part of a global economy increasingly dependent on IT technologies. However, it recognizes that there is not a single unified process through which webs of international relationships will be structured. Countries with shared close strategic or security concerns will structure their cyber-security ties bilaterally or multilaterally whereas other countries will rely on regional mechanisms as well as trading, political and economic ties as a basis. Some of the impetus for new cyber security collaboration may be provided by multinational firms operating across national boundaries or by firms with key supply chain relationships.

Other countries may find themselves beyond the reach of these mechanisms through which collaborative cyber security ties are woven; however, they may find themselves increasingly affected by concerns generated by SPAM or BOT networks or opportunistic exploitation by criminal elements of vulnerabilities in key financial or other critical infrastructure. An important focal point of this paper is how this wider circle of countries can be better enabled to cope with new challenges through multilateral initiatives of international organizations and other stakeholders.

The recommendations set forth in Part V are intended to identify how a critical mass of shared research and information resources—and capability building mechanisms—might be put in place. We develop in Part IV and Part V various other recommendations concerning how a better understanding of complex "networks" to deal with cyber risks can be developed and how different public officials, especially telecom regulators or IT ministers as well as other senior public officials including finance or economy ministers, can play an important role in improving an effective cyber security framework.

1. Pace of Technological Changes: Revolutionary Impact of IP-Technology

The challenge of dealing with cyber security risks is made more difficult because fast changing technological developments such as Internet protocol (IP)-technology are radically changing the way that backbone telecommunications services are being provided. This dynamic technological environment is creating an ever-evolving array of new security risks.

The revolutionary impact of IP-technology varies, of course, significantly from country-to-country and especially in emerging and developed economies.[5] The "connectivity" gap between developed and developing economies is being rapidly closed by extraordinary increases in mobile telephone services in former Eastern Europe countries, India and China, as well as other emerging markets. Other wireless technologies including IEEE 802.11 wireless LAN, higher speed, longer range new wireless networks known as WiMax (IEEE 802.16) as well as third and fourth generation GSM (3G/4G) developments have the potential to expand access to high-speed broadband Internet services and quickly integrate emerging economies into the high-capacity global information infrastructure.

[5] The Federal Communications Commission (FCC) in the United States has organized an on-line conference relating to the global deployment of IP-based technology. See http://www.fcc.gov/realaudio/rounds.html. For a view of the transition to IP-based network technologies, see for instance http://www.cisco.com/en/US/netsol/ns341/ns396/ns301/networking_solutions_audience_promotion0900aecd801c97b3.html and various articles and webpages on IP-convergence (e.g., http://www.totaltele.com/ip_convergence/index.shtml).

IP technology is transforming the structure and architecture of telecommunications and information services at almost the same pace in emerging and developing markets. The historic disparity in the levels of investment and penetration in the traditional infrastructure of telecommunications and information services does not mean that the impact of IP-technology will be delayed in emerging markets. It means that these markets are "green fields" for structural innovation.

Once centered around monopoly service providers—publicly or privately owned—today's ICT infrastructure depends on a much more diverse group of service providers. There is much increased interdependence between the providers of backbone services and the providers of services dependent, and often even stacked, upon such services. Furthermore, new peer-to-peer technologies allow millions of end-users to become in an unprecedented way service providers through sharing of music and other files (e.g., KaZaa).

There is increasing discussion in policy circles around the globe about Next Generation Networks (NGNs)[6]. An entirely new agenda of policy concerns must be addressed by regulators and policy-makers – many of whom are still struggling with an "old agenda" of adding competition into monopoly-dominated markets, increasing the availability of basic telephony and mobile services, and encouraging access to broadband services. But IP-driven services—like Voice-over-IP (VOIP) services and the increasing availability for the end-user of high-speed alternatives to copper wire connections—are raising questions about old policy prescriptions. They are fast changing the face of the telecommunications and ICT-sectors world-wide.

[6] Next Generation Networks: The integration of public switched networks, mobile networks, the internet, and any other data-networks to support the ubiquitous delivery of services. See "Next Generation Network Development in OECD Countries", Working Party on Telecommunications and Information Services Policy, OECD, April 2005.

2. Dealing with the "Dark Side" of E-Opportunities

Discussions at the first phase of the World Summit on the Information Society (WSIS) in December 2003 in Geneva and in follow-up activities leading to the second phase of the WSIS in Tunis in November 2005 well-document the strategic importance of ICT-services to the future development of a spectrum of economic, social, and political activities in emerging economies.[7] It is now commonplace for policy discussions to focus on the potential for e-education, e-health, e-commerce, e-finance, and e-government. Some overburdened officials labor under a portfolio of what they regard as "e-everything" concerns.

The WSIS on Building Confidence and Security in the Use of ICTs

In its Declaration of Principles of 2003, the World Summit on the Information Society concludes that 'Strengthening the trust framework, including information security and network security, authentication, privacy and consumer protection, is a prerequisite for the development of the Information Society and for building confidence among users of ICTs. A global culture of cyber-security needs to be promoted, developed and implemented in cooperation with all stakeholders and international expert bodies. These efforts should be supported by increased international cooperation. Within this global culture of cyber-security, it is important to enhance security and to ensure the protection of data and privacy, while enhancing access and trade. In addition, it must take into account the level of social and economic development of each country and respect the development-oriented aspects of the Information Society.'[8]

The World Bank and the International Telecommunication Union (ITU) have documented a very dramatic increase of new regulators around the world to facilitate the opening of markets and build-out of the basic backbone infrastructure.[9] These new regulators—along with their longer tenured counterparts—are only beginning to address

[7] For background on the WSIS, see http://www.itu.int/wsis/and http://www.wsis-online.net/smsi/classes/smsi/events/smsi-events-54163/event-view?descr_mode=long&referer=/event/events-list?showall=t (for a schedule of events and activities leading up to the WSIS Summit in 2005 in Tunis.

[8] Declaration of Principles, WSIS-03/GENEVA/DOC/0004 http://www.itu.int/wsis/documents

[9] An overview of the emergence of new regulatory bodies can be obtained through the web portal of the ITU which also describes recent ITU-activities relating to the control of SPAM and related e-security concerns. http://www.itu.int/ITU-D/treg/index.html

the potential of new Internet-based and other ICT-related services. To date, these entities have largely focused their attention of the opportunities of new ICT. They have been largely preoccupied with opportunities for increased investment in new infrastructure and new services relying on such infrastructure.

There is, also, a dark and potentially ominous side to the opportunities and promises. There are new risk factors that result from the increasing integration of information and communication technology into every aspect of how business, organizations, and governments now provide, or might in the future provide services. New opportunities and services also generate new vulnerabilities. These vulnerabilities will develop apace with new opportunities and will require increased vigilance and attention by policy-makers to cyber security-related concerns.

Phishing becomes a Global Threat

During the first half of 2005, the South African ITWEB reported major attempts at phishing. Three major South African banks corroborated the news. These events contributed to raise the awareness that phishing was not longer only a problem of rich highly industrialised nations. Below is a partial reprint of the first new report by ITWEB on the item.

Standard nets phishing sites[10]

By Iain Scott, ITWEB finance editor

[Johannesburg, 9 March 2005] - Standard Bank has shut down eight "phishing" Web sites in just four weeks. Phishing is the practice of tricking consumers into revealing their online passwords and other information by luring them to fraudulent sites that appear to be those of banks or other legitimate businesses. Consumers are usually lured by spam e-mails with subject lines like "account update needed". Herman Singh, Standard Bank technology engineering director, says all eight sites were based offshore and were spoofs of the Standard Bank site, with bogus URLs like "standbank.com" [...]

He says that although Standard Bank has no record of any of its customers losing money in a phishing attack, the bank has been tracking the phenomenon globally and has noticed a rapid increase in the frequency. While the problem has been more prevalent in countries like the US, Singh says it is finding its way to Africa too." As phishing becomes easier and enters the mainstream, the number of attacks is rising very quickly. "He adds that "phishing" kits can be bought for $270 and there are sites that present tutorials on how to phish. "As the international banks warn their customers, there is a move to targeting smaller financial institutions," he says. Standard Bank also uses other products to track sites and says the Cyota solution is merely one part of a comprehensive and integrated approach. The bank is planning later this year to launch the option of a "one-time" password. In terms of this project, a password will be valid for one transaction only, and when that transaction is complete, the user will be sent a new password for the next transaction. "We don't want to start a war and become a lightning conductor," Singh says. "We just want to protect our customers' information and sense of trust in electronic banking."[11]

3. Sources of New Threats: Blend of Hackers, Cyber Criminals, Terrorists, and High-tech National Security Strategists:

Policy makers have been concerned over a period of many years with a diverse range of potential threats, many of which are a result of the increasing integration of IT-related services into the provision of critical information infrastructure services and other public services. Concerns relating to Y2K contributed to increased public awareness of

[10] http://www.itweb.co.za/sections/internet/2005/0503091130.asp? S=Security&A=SEC&O= FRGN - 1

[11] The email and website used in this phishing attempt are reproduced on the Standard Bank's website https://www.standardbank.co.za/secure/securefaq/phishing_email_full.htm

potential cyber-related risks, which have been viewed in many countries, especially in the United States in graver national security-related terms since the events of September 11, 2001.

Since September 11, 2001, increased attention has been focused on the potential for paralyzing cyber threats including virtual attacks on critical infrastructures dependent on ICT-services—financial services, monitoring control systems for power, gas, drinking water, and other utility services, airport and air traffic control systems, logistic systems, government e-services, etc. The threats of debilitating worms and computer viruses such as Sasser, Blaster, Netsky, Welchia and Code Red have, of course, been visible for a number of years. But they may not just be driven by anarchical tendencies in an ever widening circle of virus writers, crackers, hackers, and other misguided computer professionals. The booming growth of ICT-services has itself spawned new gray and black market opportunities that well-organized criminal elements can exploit for huge financial advantage. Examples of very significant losses through "phishing" expeditions directed by criminal elements against financial institutions are well documented.(H)activists, and protestors against war actions have found ways to temporarily disrupt ICT-based services of governments and international organizations[12]. At the same time, experts in military and national security affairs have recognized, for at least the past decade, the potential significance of ICT-services as a part of military "information operations" doctrine, both in defensive and offensive terms.

4. Nature of New Threats: From Denial of Service to Attacks on Data Authenticity

New risk factors and challenges seem, moreover, to be evolving as rapidly as the spread of the high-speed Internet infrastructure.

[12]

Policymakers are concerned increasingly not merely with the potential for cyber "denial of service" attacks. They are increasingly concerned about the myriad of potential ways that the authenticity of data resources can be corrupted and basic trust in ICT-dependent services can be collapsed. For instance, there is growing alarm about coordinated and organized efforts to take over, and embed in, computers—both owned and operated by individuals and organizations—an unauthorized remote control capacity known as BOTs. BOTs can turn such computers into vehicles to attack and disable other computer systems and network components, e.g., routers, including those of critical (information) infrastructure providers as well as other important international organizations. The risk grows commensurately as more high power PCs are connected at ever higher speeds of connectivity.

5. "Weak Links" in the Global Information Infrastructure:

Concerns about cyber security cannot thus be focused only on sophisticated business and government systems in countries with an advanced infrastructure. It is, of course, critically important to focus increased resources on protecting core government and private sector resources in industrialized countries facing the highest levels of risk. Howver, there also needs to be more focus on the "weakest links" or operational environments in the virtual chain of global computer networks. This is one of the critical themes of this discussion paper.

These "weak links", which are a consequence of poor security and can occur in countries with low-bandwidth as well as with very high-capacity networks, are becoming breeding grounds for cyber chaos. They can be targeted at, and wreak havoc, on ICT-dependent infrastructure anywhere on the globe. Aggregations of poorly protected computer capacity need not be targeted at local or geographically proximate markets. Regionalism does not have much meaning in a cyber world. Because of the very global reach of the Internet backbone—and the difficulties of cordoning off national markets or identifying the source of potential threats—there is a new scope and scale to emerging cyber threats and an increased need for a truly global approach to enhance cyber security.

Potentially, any market with a combination of high capacity PCs and broadband connections can become a virtual "haven" for disruptive and malignant forces operating over the global Internet backbone. The potential risk to other markets—and to local, regional, and global businesses, private, and public services—knows no geographic boundaries and is not dependent on the overall state of ICT-development on an across-the-board basis.

It may well be that residential users—without significant protection against viruses and common maladies of today's computer environment --represent the greatest source of vulnerability to critical basic infrastructure services—such as financial services, transport, public utility, health care, government services, and core ICT-services. Thus, cyber security concerns must be comprehensive in scope. They cannot be narrowly focused on increasing security only on the core activities of government institutions or at major business enterprises and large organizations.

This complex set of linkages was the subject of a case study for this work (see Appendix A), where a multinational firm (the "host") and its supply chain were researched from a cyber-risk perspective. Among other questions, the study examined to what extent a set of firms depended on the internet to manage their supply chain, and the consequences to the host's ability to produce and ship product if the internet were to fail. One of the results of the study was the unexpected diversity of the linkages among the firms and their suppliers, and how, in the event of an internet failure, certain services such as overnight delivery become chokepoints. For example, the host firm is moving to require all supply chain communications to occur over the internet. If a supplier has privileged access to the host's internal network, a cyber security shortcoming on the part of the supplier would expose the host to attacks on its internal systems due to the linkages between the firms[13]. The host would be wise to take a broad view of information security that would take into account the linkage to the supplier (see sidebar).

If the internet were to be unavailable for a significant period of time, all the researched firms would start shipping documents using an overnight service such as FedEx. It is likely that the great majority of firms would also rely on overnight services in such a situation. Even excepting the fact that firms such as FedEx are very reliant on ICT, it is doubtful that they would be able to fully handle the increased volume of shipments. This is an example of a linkage that crosses business sectors.

There are other linkages that are completely obvious and need no comment, such as the linkage between electric power companies and most facets of life.

6. Key Questions Facing Cyber Policy-makers

The questions facing policy-makers concerned with cyber security are legion. The answers are just beginning to be developed:

How then should policymakers in the public and private sectors concerned about the development of ICT-related services respond to an environment still full of opportunity and promise yet filled with areas of potential risk?

How, in particular, do telecom sector ministries or independent ICT-regulatory bodies (as well as regulators with responsibilities for other CIIP sectors) deal with policy concerns relating to other key infrastructure sectors involving financial services, energy, health care, transport, government e-services, and other policy domains that are beyond their immediate policy remit?

[13] For an example, see http://www.computerworld.com/securitytopics/security/cybercrime/story/0,10801,98355,00.html

How should these officials better position themselves to deal with serious potential concerns dealing with criminal activity or law enforcement—or more particularly with grave potential concerns relating to national security policy? Though many established regulators have been involved with law enforcement and intelligence-related activities, many new regulators must address concerns that have traditionally been dealt with by officials in intelligence and national defense ministries in their countries.

There are other tough questions relating to the importance, in dealing with cyber security concerns, of the private sector and the international nature of the policy challenge:

How should governmental policymakers deal with the fact that an increasing number of critical infrastructures are in the hands of the (semi-)private or private sector entities and not subject to direct or indirect government or regulatory control?

How should governmental policymakers deal with the fact that these critical infrastructure operators are increasingly part of global enterprises based in other nations?

How should governmental policymakers deal with the fact that such critical infrastructures are operated via critical information infrastructures across borders of organizations and nations?

How should governmental policymakers deal with the gap between business risk and societal risk in circumstances where the real impact of critical infrastructure disruptions by cyber attacks is on citizens, business consumers, and dependent sectors and not on the critical infrastructure provider?

How should policy responses vary from country-to-country depending on differences in the current state of institutional, legal, and technological developments relating to the ICT-sector?

How can policymakers and senior decision-makers in large organizations and government deal with the international dimensions of potential cyber security concerns, especially when potential threats and incidents can involves countries that are not at all geographically proximate and can originate in countries half-a-world away?

What can be done to strengthen international coordination across national boundaries and within regions and among a hugely diverse and heterogeneous group of public and private sector entities with responsibilities and concerns relating to cyber security matters?

Ultimately, one of the most critical concerns for independent regulators is how can they deal with risk management and creating a culture of ICT-security in their sectors of responsibility?

7. Basic Rationale for Focusing on Cyber Security: Encouraging More Stable Climate for Investment and National Security Concerns

Policymakers will need to come to terms with the fact that the huge opportunities created by new ICT-related services are inexorably linked with new and dynamic risk factors.

These risk factors are critical to manage in order to create a stable climate for new investment in the ICT and related sectors. It has not always been case, of course, that what might be described as “e-risks” has been viewed as inevitably intertwined with “e-opportunities”. But this is very understandable. E-risks are highly dynamic and compounded by new technological and market developments. The more significant the revenue flows over ICT-based networks in the financial sector, for example, the greater the incentive may be for organized criminal elements to capitalize on these opportunities.

As the risks created by new ICT-based systems becomes more demonstrable, those who finance new infrastructure investments or new business opportunities are likely to insist that potential risk factors that could do irreparable harm to new assets, or jeopardize revenues streams, are effectively addressed by business risk management processes. Moreover, when societal risks exceeds business-related risks, governments will either need to accept or cover the excess risk through government subsidies or insurance schemes or will at least need to determine how much of the risk should be imposed on the business sector.

One important pragmatic rationale for attaching high priority to cyber security seems very clear. Policies to promote and attract new ICT-investment are inextricably linked with an effective policy framework for managing and addressing new risk factors.

As key sectors of domestic and closely inter-linked national economies become more ICT-dependent, they are becoming more vulnerable to acts of cyber vandalism and (h) activists, or to sinister attacks by organized criminals, terrorists, or state-sponsored initiatives intended to disrupt stable economies, societies, or political arrangements. Though the basic rationale for future cyber security policies will be to ensure a favorable climate for future investments and to protect investments already undertaken in the ICT- and related sectors, national and international security concerns are likely to loom increasingly important in the minds of policy makers. An integrated effort by the public and private sectors will be required to develop a comprehensive and highly complex set of cyber security and related policies. These policies will need to span across a range of different government ministries, independent regulators, regional and local agencies, and a multiplicity of private or semi-privately owned enterprises. They also reach inevitably across national boundaries, both regionally and globally.

Multinational firms and cyber security

Conversations with multinational firms reveal that they are well aware of the ICT risks they face as a result of doing business with firms in less developed countries. Multinationals typically have a questionnaire regarding firm cyber security practices they require potential business partners to answer; the better the firm’s cyber security practices, the more likely the firm is to get the business. Firms also pay attention to the technological and environment: just as many multinationals will not entrust high-value intellectual property to firms in countries with poor intellectual property practices, multinationals will likely not entrust business that requires high-value data to firms in countries with poor cyber security practices.

8. Complexity of the Challenge of Achieving Adequate Cyber Security: Both Regulatory and Market Forces May be Ineffective

The potential policy responses to the increasing risk outlined above need to be straightforward and be discretely focused. However, the mix of required policy initiatives is highly complex and varies from country-to-country, from industry sector-to-industry sector, and from firm-to-firm.

New institutional structures and policy coordination mechanisms can be put in place, and existing initiatives can be reinforced. Best or good practices from other countries can be adopted. At the tactical/operational level, information sharing and analysis centers (ISACs)[14] and at the operational level computer security incident response mechanisms such as CERTs may be established. However, as set forth in further detail in section III6, the webs of computer security incident response mechanisms are likely to be driven by the differing requirements of diverse enterprises, industry sectors, inter-sectoral relationships, and national economic environments. It is exceedingly difficult, if not impossible, to set up a national CERT and expect that its role and functions can be dictated on a top down basis. Managing cyber security risk is an inordinately complex process because of the extraordinary range of different entities, institutions, and interests at stake.

The potential cyber security risk factors cannot be addressed only by regulation or other traditional regulatory measures. Because of the dynamic nature of protecting against cyber risks, regulation, or even worse legislative mandates (whether in the telecommunication sector or other industry sectors) may turn out to be a blunt and ineffectual policy instrument. However, it is also unlikely that government policy-makers can confidently rely on economic or market forces alone to address a wide range of

[14] The function and organizational aspects of ISACs and CERTs are outlined in sections III5 and III6.

potential cyber threats. Some potential threats may arise because of outright market failure. In other cases, private firms may be adjusting too slowly or inadequately to a poorly articulated set of risk factors. Such risk factors may also require remedial measures too costly to undertake without more consensus by public officials and by the public, semi-public, and private sectors about the need to act. In other cases, risks to one organization or sector may require remedial measures by another organization or sector, for which the latter does not have an adequate incentive to address.

It is often said that cyber security concerns require an extraordinary new public-private partnership.[15] However, the term public-private partnership is so vague and diffuse as to entirely unhelpful to government and business leaders seeking to confront the new cyber challenges. What is required is a detailed and careful assessment of the various ways that government, public, semi-public, and private sectors can work together to manage future risk factors. This requires a clear understanding of potential institutional and structural impediments as well as of the market and other incentives necessary to encourage effective, coordinated responses to new challenges. Furthermore, this assessment needs to take into account the different levels where cooperation can occur: at the strategic, tactical, and operational levels[16] as set forth more fully below.

[15] There is abundant commentary on the role of public-private partnerships. See information collected by the OECD. This site includes substantial information about mechanisms for mobilizing public-private partnerships and for developing a culture of security. http://www.webdomino1.oecd.org/COMNET/STI/IccpSecu.nsf?OpenDatabase. See also other web sites referenced in footnotes below including http://www.enisa.eu.int/ (European Network and Information Security Agency), http://www.cesg.gov.uk/ (site on UK National Technical Authority on Information Assurance).\ http://www.niscc.gov.uk/ (UK National Infrastructure Security Co-ordination Centre), http://www.iaac.org.uk/ (U.K. Information Assurance Advisory Council), and http://www.cyberpartnership.org/ (U.S. National Cyber Partnership site with many hyperlinks and useful references to policy papers relating to cyber corporate governance, residential and business awareness initiatives). The International Telecommunications Union has also undertaken a comprehensive initiative to deal with cyber security concerns through standardization and other international collaborative activities. See http://www.itu.int/ITU-T/worksem/cybersecurity

[16] The levels and roles are derived from: Van Till, J., Luiijf, H.A.M., et al. (2001), *KWINT: Samen werken voor veilig Internet verkeer, een e-deltaplan,* Ministry of V&W, The Hague, The Netherlands. Further discussion in: Luiijf, H.A.M. and Klaver, M.H.A, “Protecting a Nation's Critical Infrastructure: The

There are also many “divides”, described below, that separate ministries and agencies, national governments, and public, semi-public, and private sector entities that might be involved in dealing with the cyber security challenges.

Effective policy depends on coming to grips with the complexity of the challenge. It requires a comprehensive and “systemic” overview of the scope of the problem of protecting ICT-infrastructures including the critical information infrastructures against the broad gamut of threats. It means that simple, seemingly straightforward policy responses at the tactical/operational level such as establishing ISACs or policy coordination mechanisms need to be put in an overall context. Each such policy measure must be seen as only a partial solution—as one piece of a complex and inter-related set of policy initiatives.

9. Key Elements of a Cyber Security Policy Framework: A Network of Many Nodes and Information Flows

Many seasoned observers of policies relating to the protection of critical information infrastructure highlight a number of critical objectives of such policies. These objectives are sometimes delineated in summary terms as four or five general objectives.

It is also useful, however to “disaggregate” some of the key aspects of an overall approach to cyber security and break them down into a larger number of separate functional elements. Underlying the various policy objectives outlined in Part II, such as assessing threats or dealing with cyber security incidents, there are some specific “processes” or “procedures” that need to be carried out in either public sector or private sector entities. Cumulatively, these various processes and procedures, viewed

First Steps”, In: *Proceedings 2004 IEEE International Conference on Systems, Man & Cybernetics*, October 10-13, 2004, The Hague, The Netherlands and in Luiijf, H.A.M. and Klaver, M.H.A., *Protection of the Dutch Critical Infrastructures*, International Journal for Critical Infrastructure Protection (issue to appear late 2005).

cumulatively, represent the various institutional and organizational arrangements that must be put in place in a comprehensive and effective set of cyber security policies.

As is explained more fully in Parts II and III of this paper, these various and diverse processes and procedures involve a set of distinct information flows relating to each of the key functional elements of a cyber security policy. These information flows can be viewed collectively as a complex "network" consisting of "nodes" or centers of decision-making with very specific information flows between and among "network nodes".

Such a "network model" can provide policy makers with a new way of thinking about cyber security policy. It can help them "visualize," or develop an overview of, the full scope of the problem of dealing with cyber security. It can help develop a common vision—shared among a diverse group of stakeholders in the public and private sectors—of a series of policy options or initiatives that need to be considered in order to address key cyber security challenges on a well-integrated and coordinated basis.

Such a network model has the further advantage of being "institutionally neutral". Because it focuses on key functional elements of an overall cyber security policy and on "processes" and "information flows", it makes no assumptions about, and is not based on any predilections concerning, any preferred set of institutional arrangements. Given the significant diversity of cultural, legal, and institutional traditions involved in emerging markets, this is a critically important matter.

The dynamic nature of a network model is very likely to focus policy-makers on incentives and disincentives to information flows. It should allow them to bear down on how a mix of market-based pressures, laws, regulations, directives, and policies can shape the ways that risk factors are identified, analyzed, and acted upon. It can highlight how various institutions and economic players are likely to respond to, and manage, risks to maximize their differing perceived financial, political, and other societal interests. An assessment of the "performance" of such a "network model" is analogous, in some respects, to how traditional economic markets are analyzed by economists and financial analysts. However, cyber security networks involve a complex set of “market signaling” and incentive/disincentive relationships. This complexity results from the fact that key interactions and relationships straddle both economic, as well as politically motivated, participants in the “cyber network system”.

Because the network model described above is institutionally neutral, it necessarily means that various key elements of an overall cyber security policy will be implemented in practice through a very diverse set of institutional arrangements differing from country-to-country. Countries at different stages of development will have differing perspectives on the overall vulnerability of their own critical information infrastructures. They are likely to be at different stages of setting up overall policy coordination mechanisms. Some sectors including the financial services sectors may be further along in addressing potential risk factors given interdependencies with international clearing, central banking, and financial market systems where cyber security concerns are accorded high priority. Other emerging economies with fast-growing ICT sectors involved in software development or outsourcing such as the Indian economy may be according higher priority to cyber security concerns because of global supply chain relationships as well as national economic policy.

CERT organizations may be at different stages of development—some newly established, others with longer standing and well-developed collaborative ties with CERTs in neighboring countries. These CERT organizations may be at different stages in developing ties within industry sectors, with large enterprises, and with government agencies. In turn, they may be still evolving their own relationships with the independent telecommunication regulators and national security agencies as well as their connection to homeland security coordinating mechanisms.

In short, there is nothing that is static or uniform about how cyber security-related “networks” are structured or evolving. They are, in fact, growing in an organic fashion-- like neural ganglion-- developing to deal with new pressures and demands from the public, semi-public, and private sector alike. The very complexity and diversity of new arrangements and structures represents a challenge to national and international policy-makers concerned with cyber security. There is no simple, hierarchical way that linkages are likely to develop among CERT or CSIRT organizations within a country, or on a regional or international basis as is described in detail in section III6.

The discussion in the next part – along with the diagrammatic representative of the network model described in Part III of this paper –-is intended to highlight specific mechanisms and policy initiatives for dealing with cyber security concerns. However, it is important initially to identify key components or elements of a cyber security framework which involve, as noted above, implicit processes or procedures which will be further delineated in Part II below.

III Overview of Key Elements of an International Cyber Security Framework

Key elements of a cyber security framework are the following:

- prevention of debilitating damage and minimization of the risk of cyber attacks;
- assessment of the potential range of threats;
- assessment of vulnerabilities of critical information infrastructure;
- improvement of information security risk management techniques in the public, semi-public, and private sectors;
- improvement of information sharing on both a formal and informal basis among key stakeholders from public, semi-public, and private sector entities, among private sector entities within and across sectors, among intelligence-related and law enforcement entities and other agencies concerned with cyber security, among public agencies and the private sector including the public at large;
- development of mechanisms to respond to cyber incidents;[17]
- improvement of regulatory tools and mechanisms for minimizing the risk to basic (tele)communication, ICT-controlled, and other information services;
- development of effective law enforcement tools to analyze hacking incidents and systems used in attacks (inforensics), to impose penalties and sanctions in the event of cyber security incidents;
- development of effective tools against cyber attacks;
- improved quality of system and application software;

[17] A cyber security incident requires first the detection of an anomaly or known ‘fingerprint’ of a threat. Such alarms, after sequencing and correlation, may generate an incident which needs to be analyzed and acted upon. From the determination of the intent of an incident - if that is feasible – one could decide that the incident is deliberate action, allowing it to be classified as a cyber attack.

- coordination of cyber security initiatives among public, semi-public, and private sectors;
- monitoring the performance of the cyber security initiatives and make changes as required;
- outreach initiatives to involve all key stakeholders;
- effective international coordination among public, semi-public, and private sector entities involved in the cyber security framework.

The discussion below highlights each of these key elements of an overall approach to dealing with cyber security concerns. Each of these key elements deals with an area of policy concern that is an integral part of an overall strategic framework for protecting critical information infrastructure from cyber-related risk. In addition, the discussion of each of these elements of the cyber security framework described below also identifies some of the institutional and policy-related mechanisms that are of critical importance in implementing the elements. It also identifies some practical, operational steps that policy-makers may be required to take in order to effectively implement an overall cyber security policy framework. We discuss below some of the "nuts and bolts" processes and procedures that under-gird each of the key elements of an overall cyber security framework.

1. Prevention of debilitating damage and minimization of the risk of cyber attacks

One of the critical objectives of an overall cyber security program is the prevention of debilitating damage to critical public, semi-public, and private sector services. Such critical services are essential to national economies and to maintaining public confidence in the effective functioning of the public, semi-public, and private sectors.

This does not mean that all cyber attacks or incidents, and all economic damage can be prevented. There may even be some basic differences of perspective about what level of protection is adequate. Public officials concerned with crisis management and emergency preparedness may be focused primarily on maintaining critical economic and public sector services. Business executives may be concerned about a more targeted and focused level of protection, i.e., preventing significant economic or financial damage to their enterprise or to the markets in which they operate. There will inevitably be some differences in priorities about how public resources and energies to respond to potential cyber security incidents should be allocated and targeted.

There is likely to be, of course, a strong consensus that national policies should be structured to minimize the potential cyber security risk facing countries. To make such a core objective feasible and practicable, however, may require a significant effort to achieve broad consensus concerning the importance of more extensive and effective reliance on cyber risk management techniques and of improving cyber-related risk management on an across-the-board basis in the public, semi-public, and private sectors.

Beyond the actual risk management techniques are the types of risks that the continuum of public-private entities pay attention to. As noted above, business executives and public officials may be interested in different types of risk. With respect to critical infrastructure, to a large extent the private sector’s interests are aligned with those of the public sector: if critical infrastructures such as transportation, energy and telecom are not functioning, the firms involved in those infrastructures are not making money.

At a practical level this means that such firms are inherently incented to consider and minimize their business continuity risks. How effective these incentives are at making critical infrastructures secure has much to do with how inclusive individual firms are in considering what events would impact them, in essence, defining what is an “adequate” level of information security. Risk management techniques will allow business executives as well as public officials to make this judgment in a rational manner.

Risk management is, of course, not a discipline unknown to public, semi-public, or private sector leaders throughout the world, but its application in the area of cyber security is still in the early stages according to the opinion of many experienced observers in the business sector, even in many advanced countries and large corporations. This is particularly true because essential data needed to be able to correctly estimate risk and to manage it is often lacking. A number of European governments have, of course, developed and applied risk methodologies in assessing the risk for critical infrastructure sectors of their economies. Many financial organizations are developing sophisticated risk assessment procedures on a firm and sector-oriented basis. Nevertheless, there is significant need to improve cyber security risk appraisal procedures and to elevate their importance with senior executives and corporate boards. Moreover, there are new and complex dimensions to potential cyber security threats and vulnerabilities that may require many changes in past risk management practices in the public, semi-public, or private sector. Often, current methodologies result in analysis reports that are too detailed and too technical and are not presented in terms that can be easily assessed by senior management. Fast-moving ICT-developments introduce new features and product cycles which may be vulnerable because security features are not built in or are available on a timely basis. It also may be necessary to pursue many new policy initiatives including unprecedented cooperation among the public, semi-public, and private sectors as well as new levels of multilateral collaboration.[18]

2. Assessment of potential range of threats

The assessment of the potential range of threats is, of course, a critical element of any comprehensive program to manage cyber-related risk. If threats do not seem to be tangible, credible or imminent, any effort to commit substantial public, semi-public, or private resources in response to such threats will be difficult to mobilize.

[18] See, for example, an assessment of the top-20 vulnerabilities of information networks assembled by the SANS (SysAdmin, Audit, Network, Security) Institute (http://www.sans.org/aboutsans.php). Their study of network vulnerabilities can be found at www.sans.org/top20/ The SANS Institute organizes a series of webcasts on network security issues. Its web site includes many useful hyperlinks on cyber security.

Cases of damages arising from worms and viruses launched by a diverse collection of hackers are well known and documented. Nevertheless, worm damage cited in the media is often highly speculative and not based on solid numbers. This fact discredits the threat of worms in the eyes of many decision-makers. Specific examples of outages due to worms make a more powerful statement. However, it is harder to document other potential threats. Such threats can arise from organized criminal elements, (h)activists, protestors against war or other activist actions, terrorists, or even from nation states. This latter type threat may be as a part of open or covert information operations by military/national security-related entities, or by (h)activists, terrorists or criminal elements harbored by rogue or failed nation-states.

There was, of course, even prior to, and then following, the events of September 11 a readiness by various governments to anticipate a wide range of potential cyber-related attacks. Some observers described the scenario of an "Electronic Pearl Harbor" based on comprehensive and debilitating denial-of-service attacks. Assessments of potential threats have, in recent years, become more refined. Although (h)activists regularly have used denial-of-service and other attacks on organization, governments, and disliked businesses, there is some skepticism about the motivations specifically of terrorists groups in using such means.[19] It is not apparent to some observers why virtual attacks on infrastructure might be preferred to the obvious and disruptive impact of attacks directed against physical infrastructure. The sobering attacks on commuter trains in Madrid on March 11, 2004 underscored the devastating impact of brutal and senseless attacks on innocent members of the public. The public can barely grasp the even more catastrophic damage that might be inflicted by biological, chemical, or radiological weapons, e.g. a dirty bomb. Such catastrophic risks to tens of thousands of people and civil order with short and long term effects has no doubt reduced the priority attached to

[19] For example: Weimann, G. (2004), *Cyber Terrorism: How Real is the Threat?*, Special Report 119, U.S. Institute of Peace (http://www.usip.org/reports).

technologically driven and abstruse types of attacks on critical information infrastructure. Yet the basic lesson of September 11 remains: scenarios for attacks that are seemingly unimaginable and improbable remain critical to address.[20] Actually, one observer has warned that, paradoxically, 'the success in the "war on terror" is likely to make terrorists turn increasingly to unconventional weapons such as cyber terrorism.'

The potential scope of risk is not limited to attacks that immobilize or critically damage information infrastructures including the Internet itself.[21] In fact, because the Internet offers some very effective tools for planning and command and control of terrorist operations, and is used for, e.g., fund raising and recruiting[22], the most radical and unprincipled terrorist groups in the world may arguably have an interest in protecting this resource but in exploiting its vulnerabilities on a very selective and strategic basis.

Increasingly, the Internet is an ever more important avenue for finance and commerce. It is creating at the same time a cornucopia of financial opportunities for organized criminal elements. Phishing, pharming,[23] and other criminal practices that are intended to corrupt or economically exploit high-value data resources are becoming part

[20] This is especially true as the U.S. makes it harder for terrorists to gain physical access to targets, and the next generation of terrorist recruits becomes more versed in cyber attack techniques. For details on the cyber capabilities of terrorist organizations see: 'Examining the Cyber Capabilities of Islamic Terrorist Groups', Technical Analysis Group, ISTS, March 2004 - http://www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf.

[21] For information relating to threats as seen by the financial services sector see information on the web site of BITS, a roundtable of financial service sector enterprises, www.bitsinfo.org/bsit.html .

[22] Weimann, G. (2004), *How Modern Terrorism Uses the Internet*, Special Report 116, U.S. Institute of Peace, March 2004.

[23] *Phishing* is the act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. *Pharming* seeks to obtain personal or private (usually financial related) information through domain spoofing. Visit http://www.antiphishing.org/ for trends and counter measures.

of the basic tradecraft of a global “black economy”.[24] This black economy mirrors and grows exponentially with the “legitimate” e-economy. This black e-economy can generate financing for terrorism[25] or offer “off-budget” funding to flow into the interstices of the military, police, or national security apparatus of nation states. Thus, suppressing the growth rate of the black e-economy protects businesses and individuals from sophisticated criminal activity. It also provides increased domestic and international stability and security by cutting down, or off, funds that might be used aggressively and nefariously.

It is exceedingly difficult to appraise the size of, and scope of risk presented by, a cyber black economy. This is specially so with respect to the potentially hostile involvement of nation-states in this activity. Some recent surveys have attempted to document on the basis of the public record (sometimes with “grey” sources relying on intelligence agencies) the information operations (“cyber warfare”) intentions and capabilities of a range of nation states.[26] These nation states have had traditionally a significant military or national security presence in the international arena. Alternatively, a number of countries have been identified by the United States and allied countries, as potential rogue or renegade states threatening international stability. A comprehensive list of nation states that figure in emerging discussions of ”cyber warfare” in offensive or defensive terms includes, inter alia, North Korea, Iran, India, Pakistan, the People’s

[24] ‘Phishing Feeds Internet Black Markets’, Brian Krebs, Washington Post, November 14, 2004 – http://www.washingtonpost.com/wp-dyn/articles/A59347-2004Nov18.html

[25] For example, Imam Samudra, convicted and sentenced to death for planning the 2002 Bali nightclub bombings in Indonesia, recently released his memoirs. In his book, he urges Muslims to engage in cyberjihad against American computer systems, particularly for credit card fraud, and provides a primer on how to commit cyber crimes. See ‘An Indonesian's Prison Memoir Takes Holy War Into Cyberspace’, Alan Sipress, Washington Post, December 14, 2004 - http://www.washingtonpost.com/wp-dyn/articles/A62095-2004Dec13.html

[26] See ‘Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States’, Charles Billo, Welton Chang, ISTS, December 2004 - http://www.ists.dartmouth.edu/directors-office/cyberwarfare.pdf

Republic of China, the Russian Republic, as well as the United States, Australia, Sweden and some NATO member nations.[27]

The difficulties with public surveys in this area are clear. They necessarily depend on public sources, often on dated information. As such, they could fairly be viewed by skeptical, business-oriented observers as an almost useless contribution to any credible threat assessment effort. Such surveys do, however, establish that there is a "less visible" component to any overall threat assessment. This component must somehow be factored into any effective overall risk management strategy.

Policy-makers, especially in the private sector, often dismiss the importance of assessing threats, as opposed to evaluating vulnerabilities, as a critical part of a national cyber security policy. They do so on the ground that it is inherently difficult to substantiate and quantify risk factors in an open and transparent democratic society and in a world that is replete with "potential threats" to international stability and security. It is easier, of course, to focus on more tangible, manageable, and knowable elements of cyber security such as vulnerability assessments. Nevertheless, there is likely to be significant urgency in developing credible "intelligence assessments" of potential threats. These assessments would synthesize the best available, most recent and credible information in the hands of national intelligence services for use in a range of public, semi-public, and private sector deliberations with respect to cyber risk management.

We discuss in further detail below in Part IV, the specific ways and means by which intelligence material can be synthesized and shared within the international community—and especially with the private sector. The intelligence assessment process required to deal with cyber security issues is a novel and challenging one. It is arguably significantly different from the assessment process applicable to past and more

[27] Hostile cyber actions between India-Pakistan, Azerbaijan-Armenia, Japan-People's Republic of China have taken place in the past.

conventional threats to international security. In both cases, of course, intelligence agencies are involved in shifting through, and extracting, data from satellite or cable data streams on backbone international infrastructure. However, it is likely that significant threat indicators may only emerge from accumulating, correlating, and analyzing incident-related data[28] that may become visible only through detection on a decentralized basis at the enterprise level or through analysis of information collected through a range of CSIRT mechanisms in one or more countries.

3. Assessment of vulnerabilities of critical information infrastructure

Given the difficulties of assessing the potential threats to critical infrastructures, policy-makers have focused significant attention on potential areas of vulnerability of critical information infrastructures in their countries.

The first step in this process has been to identify various critical infrastructure sectors and their critical services. There are differences in how critical sectors are classified by various countries. However, there tend to be some very common approaches. For example, the telecommunication sector is, along with the electrical power service (energy sector), the bedrock upon which almost all other critical public, semi-public, and private sectors and their critical services are dependent.

The financial services sector generally gets a top billing on the list of vulnerable critical information infrastructures. There is, as is discussed below, heightened concerns about ICT-control and monitoring systems, or so-called supervisory control and data acquisition (SCADA) systems for electrical power, gas, oil, sewage, and drinking water infrastructure.

[28] An example is the Norwegian early warning system VDI experiment (source: http://www.ddsi.org/Documents/CR/norway.pdf).

The World Bank has undertaken a major effort to assess the risk factors and vulnerabilities of the financial sector.[29] It has also established a major, multi-prong program to educate and inform financial sector executives as well as financial sector supervisors about how to manage cyber risk and deal with potential new threats. The path-breaking studies commissioned by the World Bank provide important benchmarks that can, and should, be relied upon by leaders in other sectors. In particular, the recommendations of the World Bank study focus on a multi-layered security framework for financial institutions. This framework anticipates that security checklist requirements and liabilities can be imposed on backbone service providers as well as other key participants in supply chain relationships. The recommendations raise the important questions relating to whether focusing more attention on the liabilities of service providers might improve overall levels of cyber security in sectors that are dependent on backbone ICT infrastructure or system-related software. The World Bank recommendations highlight the extraordinary importance of clarifying the roles and responsibilities of underlying service providers and other business partners of financial institutions.

This multi-layered framework developed for the financial services sector offers a useful template that can, and should, be applied in other industry sectors, especially those that are subject to different forms of regulatory oversight and may have critical operational or supply-side relationships. These two factors can create a "hook", and

[29] The World Bank has established a web portal which includes a wealth of resources and hyperlinks with respect to financial security e-security issues. Furthermore, the World Bank has organized several web-cast seminars (http://www.worldbank.org/wbi/B-SPAN/sub_electronic_safety.htm; http://www.worldbank.org/wbi/B-SPAN/electronic_safety/sub_electronic_safety_index2.htm)relating to financial security policies which can be accessed through the World Bank portal. http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/9f941053fd4293dc852569510022c5a0/77768cb67681ae7c85256d09005807df?OpenDocument. In addition, the World Bank has prepared a number of policy studies which are available at [include web hyperlink on the World Bank E-Security Portal we will create for the project]. See http://wbln0018.worldbank.org/html/FinancialSectorWeb.nsf/SearchGeneral?openform&E-Security/E-Finance&Presentations

provide leverage, for increasing the visibility of cyber security concerns at the enterprise level. Whether it is a sector-specific regulator or ministry or a key participant in a supply chain relationship (customer or key supplier), these entities are critical points in the "networked relationships" that determine the level and adequacy of cyber security. They can be utilized in a strategic way to improve the cyber risk management across a spectrum of commercial and contractual relationships.

Other sectors that are commonly agreed to be heavily dependent on the telecom (fixed telecommunications, mobile telecommunications, satellite, broadcast) and electrical power sectors, navigation services[30], and their own critical information infrastructures are various transport services (air, rail, road, sea, river, pipelines), government sector (e.g., e-government, justice, administration, law enforcement, social services), emergency services, and human needs (e.g., drinking water, food/agriculture, sewage, health services). [31] [32] The power industry relies heavily on SCADA systems to manage and control power generation and distribution. Major rail and air transport systems use networked computers to coordinate and manage the flow of people, goods and services in a country and cross-border, etc.

Notwithstanding their differing approaches, national policy-makers have honed in on the industry sectors facing the most significant level of risk. They have all tried in differing ways to mobilize energies and institutional mechanisms in each of these sectors to confront potential risk factors. This has, in a very limited number of countries,

[30] e.g., global navigation satellite systems as GPS and the future European Galileo.

[31] See discussion in the 2004 CIIP Handbook referred to below as well as the web sites of various ISACS including http://www.fsisac.com/ (financial services); http://www.ncs.gov/ncc/main.html (telecommunication services); http://www.esisac.com/ (electric power services)

[32] Luiijf, H.A.M., Burger, H.H., Klaver, M.H.A. (2003) Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten (managementdeel). Critical Infrastructure Protection: Quick-scan of critical products and services – management report. TNO-report FEL-03-C001, The Hague, The Netherlands.

involved a “top down” effort to identify any “cascading risk factors,” i.e., circumstances where blockages or break-downs in one critical service or sector have spill-over consequences for another critical service. These spill-overs can involve risk spreading from one service in a sector to other services in that sector, or from one sector to other sectors. There are well-documented and sometimes divergent methodologies for identifying potential damaging risk scenarios.[33] The analysis relies, in some cases, heavily on intuitive or common sense assessments of potential cascading effects. There has also been, and continues to be, a major effort to develop computer-based simulations that analyze potential areas of vulnerability and diverse scenarios for cyber attacks. Such top-down analyses have very often been led by entities in national governments with the responsibility to coordinate national cyber security policies.

Though there have been efforts to identify theoretical spill-over effects, it has been difficult to develop significant operational experience and capabilities in handling potential cascading consequences of cyber risk. For example, a major cyber security exercise in the United States involved attacks that were “compartmentalized” for purposes of the exercise within specific sectors and did not evaluate procedures and methodologies for handling attacks or incidents with concurrent impacts on multiple sectors.[34] As noted elsewhere, exercises can be a significant tool for developing and improving the overall cyber security framework. See Part IV.

The locus of central coordination varies from country-to-country. A coordinating point is often established through an inter-agency committee at cabinet level in

[33] The 2004 CIIP Handbook and other relevant reference materials prepared by the Swiss Federal Institute of Technology can be found at http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdfhttp://http://www.isn.ethz.ch/crn/publications/publications_crn.cfm?pubid=224 . These materials provide extraordinarily useful country case studies and other materials on differing approaches to risk management undertaken by national, regional, and international organizations.

[34] See e.g. http://www.iapplianceweb.com/story/OEG20031202S0038.htm

parliamentary forms of government. In the United States, cyber-security responsibilities have been vested in an agency of a cabinet level department, the Department of Homeland Security (DHS). In other countries, depending upon the assignment of roles and responsibilities on a national basis, these critical responsibilities are in the hands of officials of some ministry, e.g., a Ministry of the Interior or Economic Affairs[35]. These officials frequently share information with their foreign and domestic intelligence agencies and/or law enforcement officials.

Through these institutional arrangements, various countries have sought to mobilize efforts to protect key government information infrastructure. It has proved to be a more demanding task to focus resources on the protection of critical information infrastructure which is generally subject to private ownership or control. The potential challenges of assessing vulnerabilities of CII enterprises depends heavily on differing national approaches to ownership and control of key areas of economic activity.

In some countries with a long tradition of state involvement or ownership in key infrastructure sectors, risk assessment in state-owned companies may be seen as a core governmental responsibility. It may also be given little weight. The existence of diverse stakeholders in the corporate governance process, especially private shareholders, often can result in a more independent and thorough evaluation of potential risk. This is especially the case where the major or controlling shareholders and boards of directors must take into account their potential liability to other shareholders with respect to unaddressed or undisclosed threats.

The conversion of state-owned enterprises into publicly held companies usually results in more detailed and careful risk assessment as a direct consequence of corporate law or financial market-related disclosure requirements. Even in the case of some newly privatized companies, however, historic close relationships with the state as the

[35] In Switzerland, part of this task is with the Ministry of Finance.

controlling shareholder can significantly influence the expectations and patterns of collaboration between government officials responsible for cyber security and the executives of (semi-)private or private companies either operating or depending upon critical information infrastructures. There are potentially significant differences in the ways in which corporate executives in, for instance, the U.K. or another country might deal with officials responsible for cyber security compared with their corporate counterparts in the U.S.[36] U.S. executives may often be likely to take a more skeptical, arms length posture with respect to government officials. By contrast, against the backdrop of a long tradition of state-ownership and control, officials in the French government responsible for cyber security are likely to take a much more top-down, state directed approach to dealing with cyber security risk factors. Longstanding traditions and patterns of state control and oversight are hard to uproot. For example, government accounting offices address unmanaged risk in government agencies or state-owned entities in reports to the public.[37] These traditions and patterns of governance of state-owned companies often will determine the degree to which government officials are prepared to entrust responsibilities for assessment of vulnerabilities and risk management to corporate executives and to follow a more bottom up approach to risk management.

Whatever differences in approach to assessment of vulnerabilities there may be, policy-makers adopt a consistent refrain about developing effective public-private

[36] Cyber security is managed through a cabinet co-ordinating committee in the United Kingdom, the National Infrastructure Security Co-ordinating Centre (NISCC) which brings to bear the resources of a number of ministries such as the Department of Trade & Industry as well as intelligence-related entities including GCHQ and MI-5 under a single umbrella. NISCC (http://www.niscc.gov.uk/) has engaged in active collaborative relationships with critical information sectors as well as coordinating bodies such as the UK Information Assurance Advisory Council (http://www.iaac.org.uk/). NISCC has been actively involved in efforts to develop a common international framework for dealing with cyber security issues. See http://www.niscc.gov.uk/warp_publications/intro.pdf as well as additional materials included in the proceedings of an October 2004 e-security conference organized by the Dutch Government in its role as President of the European Commission. See http://www.e-security-eu2004.nl/and related background material.

[37] An example is the U.S. Government Accountability Office (http://www.gao.gov/).

partnerships to deal with cyber security threats. There may be differences in how such public-private collaboration is implemented in practice, for example, in the U.S., the U.K., Australia, the Netherlands, or Switzerland. But there is a common recognition that government cannot act effectively without engagement and cooperation from the private sector. The degree of reliance upon risk assessment within the corporate sector may, however, differ in significant respects from country-to-country.

4. Improvement of risk management in the public, semi-public, and private sectors

Effective risk assessment and management is generally viewed as one of the key factors in having a well managed, profitable enterprise.[38]

Risk management is critical to enterprises that operate in highly competitive markets and are expected to meet rigorous basis financial performance targets that investors can rely on. Publicly traded firms have rigorous methodologies for tracking revenues and expenditures and for anticipating factors that might adversely affect financial projections.

These financial reporting mechanisms have, however, been subject to rigorous review and oversight as a result of financial scandals that in recent years have adversely affected a number of public traded firms including Enron, WorldCom, and others. As a consequence of the enactment of the Sarbanes-Oxley Act[39] in the United States following a spate of financial scandals, the entire process of reporting and disclosing financial results within many firms operating on an international basis has been made more

[38] There is substantial background information available about risk management in the IT sector as well as corporate governance procedures to deal with such issues. See, e.g. the web site of the Information Audit and Control Association, http://www.isaca.org/template.cfm?section=home, which includes an overview of IT corporate governance concerns, http://www.isaca.org/Template.cfm?Section=Governance&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=19&ContentID=47.

[39] http://www.sarbanes-oxley-forum.com/

accountable with clearer responsibilities imposed on senior management and corporate boards to "deconstruct" and review the entire financial reporting system and to take increased responsibility for the accuracy of these results.[40] Corporate executives also must identify and disclose to shareholders and the public at large a wide range of risk factors of both an operational and strategic nature. Even before public attention on corporate disclosure and accountability mechanisms increased dramatically, for example, public companies were routinely reporting potential risk arising from the so-called Y2K vulnerability of financial reporting and information systems.

There are, of course, differences in mechanisms of corporate accountability from country-to-country. However, there is general acceptance of the principle that risk factors that are not disclosed or adequately disclosed and then result in financial losses or related setbacks to the financial prospects of an enterprise can result in financial liabilities to corporate executives and board members. Financial disclosure and accountability systems can, therefore, create significant pressures for senior management and corporate boards to undertake a rigorous process of risk evaluation and then, where appropriate, to take various initiatives in response to these risk factors.

In a post-Sarbanes-Oxley environment, there is an increased expectation that corporate disclosure procedures will be better documented and subject to senior level review. New corporate disclosure requirements have resulted in a mandatory detailed bottom-up review of the various cost and revenue reporting systems on the basis of which financial statements are prepared, internally reviewed, and audited. Part and parcel of a more rigorous approach to financial reporting are better systems of risk assessment and management.[41] Improving corporate governance mechanisms has thus become a major

[40] For an overview of the Sarbanes-Oxley Act, see http://www.sec.gov/spotlight/sarbanes-oxley.htm and http://www.pwcglobal.com/Extweb/industry.nsf/docid/FE7E76BBFAFBDCA185256CE000768BF9

[41] An elaborate methodology for undertaking an assessment of cost assessment and internal controls was established by the Committee of Sponsoring Organizations (COSO), or the so-called Treadway Commission. This methodology for assessing risks in financial control systems and especially the IT-

concern of CEOs, Chief Financial Officers (CFOs), Chief Information Officers (CIOs), as well an array of other executives concerned with the information systems central to the financial reporting system.

There are, of course, significant differences in the requirements for, and the priority attached to, corporate governance and financial reporting even in countries with developed financial markets. National corporate and regulatory requirements for corporate governance and financial reporting differ, of course, from country-to-country. However, as a result of increased global financial inter-dependence and the fact that major corporations in a diverse range of markets including Russia, China, Korea, India, South Korea are accessing capital markets outside their domestic markets on a ever more frequent basis, it is expected, if not required, by financial markets, that publicly traded corporations will adhere to more rigorous corporate governance and disclosure mechanisms, especially after the Sarbanes-Oxley Act.

Such increased focus on governance, disclosure, and corporate risk management has important implications for policy-makers concerned with the emerging cyber security threats, especially those faced by private or (semi-)private operators in critical information infrastructure sectors. In principle, the same governance practices might be expected by the public of critical information infrastructures operated by the public sector. However, in practice the governance practices of public, semi-public, and private sector entities have been shown to diverge in significant respects.

related aspects of such systems may provide a useful basis for a more disciplined approach to IT-related cyber security-related risks. See http://www.coso.org/publications/executive_summary_integrated_framework.htm. These linkages are recognized in recent analyses undertaken by the Information Systems Audit and Control Association. See http://www.isaca.org/Template.cfm?Section=Governance&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=19&ContentID=47 and http://www.isaca.org/AMTemplate.cfm?Section=Sarbanes-Oxley2&Template=/ContentManagement/ContentDisplay.cfm&ContentID=11247

Corporate disclosure mechanisms and requirements can thus become a means of ensuring that on an enterprise-by-enterprise basis there is a more focused and reliable process of assessing emerging risk factors, especially in privately owned CII firms.[42] In this respect, policy-makers concerned with cyber security may be working with, not necessarily against, market expectations.

It is also right to assume, of course, that, in the rigorous and competitive conditions of national and global financial markets, firms will be inclined to reduce or eliminate expenses that are not materially and significantly contributing to the bottom line performance of the firm. Thus, advocates of risk reduction in a firm, who seek higher levels of expenditures for security-related systems and technologies, may find themselves confronted by financial executives or senior managements anxious to improve financial results. These pressures will tend to operate, across national markets, penalizing those firms that may adopt more risk adverse strategies.[43]

Some of these market pressures against risk adverse management can be mitigated where policy-makers can effectively make the case that additional security-related initiatives are a matter of overriding public concern.[44] Executives will be expected to take these matters into account in their overall strategic approach to their operations. As a consequence of increased public awareness and government initiatives to raise the profile of cyber risks, executives from the public, semi-public, and private sectors might well be expected to take more careful account of such cyber security concerns. Moreover,

[42] Various background materials on IT corporate governance procedures are provided at http://www.isaca.org/Template.cfm?Section=Governance&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=19&ContentID=47

[43] To paraphrase a cyber security executive at a multinational firm, "Nobody's rewarded for good cyber security, but they are penalized for bad cyber security."

[44] From: Luiijf, H.A.M., *Critical infrastructures and consequences for industry*, 2nd Handelsblatt Conference on Security Policy and the Defence Industry "Security as a Global Challenge", 12-13 April 2005, Berlin.

cyber security concerns, like quality-of-service related issues in an earlier era, are increasingly likely to become viewed as an integral aspect of a “product” or “service,” rather than as a separate matter of “regulatory” concern. Thus, public dialogue as well as better information and data relating to cyber security concerns from a variety of public, semi-public, and private sources can reconfigure the way that corporate executives perceive areas of risk and provide core business services. The very process of focusing increased public and corporate attention on potential areas of corporate and societal risk can indirectly and subtly influence the substantive and procedural priority that attaches to the appraisal of such risk factors.

From a public policy standpoint, it is likely to be very constructive and effective to raise the profile of the cyber security risks in the context of the provision of core services provided by critical information infrastructure sectors. It is also important to focus more attention on the corporate governance mechanisms through which such risks are actually evaluated.

There is, of course, an enormous amount of analysis and assessment of what are often described as ICT corporate governance procedures.[45] This analysis addresses in detail the intra-corporate dynamics of the risk appraisal and management process. It deals, for example, with the reporting and accountability relationships of executives concerned with managing the ICT-infrastructure and those with responsibility for assessing any risk factors that may be created by such infrastructure. The former group of executives may have, in many corporate structures, direct reporting and managerial relationships with CFO’s or other senior executives responsible for the bottom line performance of an enterprise. In turn, CIOs may have oversight and control

[45] See Information Security Audits and Control Association www.isaca.org; Octave (Operationally Critical Threat Asset Vulnerability Evaluation)—Risk Assessment Methodology of U.S. CERT, http://www.cert.org/octave; Rand Corporation—Engaging the Board: Corporate Governance and Information Assurance, www.rand.org/publications/MR/MR 1692/MR 1692.pdf; Comprehensive Risk Analysis Network, Swiss Federal Institute of Technology, http://www.isn.ethz.ch/crn.

responsibilities for executives responsible for assessing and managing risk inherent to the various information infrastructure activities.

The process of clarifying corporate governance relationships might result in reassessing corporate accountability relationships.[46] CEOs or board members might be expected to make independent assessments of cyber security concerns that might be the basis for securities-related disclosure to investors or for other types of reporting to public officials or industry structures (potentially also informal groups of senior executives) with responsibility for enterprise and sector-related security issues. Modifying or redirecting the flow of information and risk assessments with respect to cyber security issues may fundamentally affect how effectively such security concerns are dealt with by the firm and within its various commercial or sector-related relationships.

There are a number of different ways in which the flows of information relating risk management might be modified or redirected. One obvious step is, as noted above, to elevate the corporate level at which risk is evaluated and to require additional documentation or substantiation with respect to such risk analyses. Another is to authorize, if required, more informal gathering of risk-related information from peer firms. Such inter-firm communications might be discouraged for legal, competitive, or commercial reasons. For example, private companies that have provided sensitive information to the government may find that information subject to public disclosure based upon freedom of information laws existing in many countries. Alternatively, exchanges of information may also run afoul of anti-trust or competition laws or concerns by financial or securities regulators about the exchange of sensitive competitive information among enterprises.[47] Some countries have studied, or are studying, ways to

[46] See “Engaging the Board: Corporate Governance and Information Assurance”, a RAND Corporation policy paper, http://www.rand.org/publications/MR/MR1692/

[47] See recent U.S. SEC policies in the financial sector relating to inter-firm information sharing.

remove such blockages through amendments to freedom of information laws as was the case in the United States.[48]

A way ahead may be to develop cyber corporate risk management capabilities – through a diverse range of managerial and institutional approaches described more fully in Part III --that improve risk assessment and management in significant ways.[49] Such information could be gathered from a range of supplier-related sources — from backbone infrastructure or internet service providers, from equipment and software suppliers, as well as from various independent "specialist firms". As awareness of potential cyber-related risk increases, various third party security consultants and advisors are becoming an additional source of know-how and expertise for many firms.

In addition, there may be emerging opportunities for third parties such as insurers with highly specialized experience and expertise in the global security field to establish, in effect, a market for risk reduction initiatives.[50] Such firms are likely to be able to provide procedures and disciplines to implement multi-layered security procedures. Such

[48] Section 214 of the U.S. Homeland Security Act, enacted in November 2002, contains a series of provisions aimed at promoting the flow of sensitive information about the nation's critical infrastructure to the federal government for homeland security purposes by exempting "critical infrastructure information" that is voluntarily submitted to DHS by private-sector industries and other nonfederal entities from FOIA disclosure. See U.S. Department of Justice Office of Information and Privacy FOIA Act Post - http://www.usdoj.gov/oip/foiapost/2004foiapost6.htm

[49] As example, Dutch banks have entered into arrangements for the exchange of information on fraud techniques and actual fraud cases as that is a threat seen for the whole financial sector. Based upon such, model cyber threat information will be shared and not be regarded as competitively sensitive information.

[50] See the SANS Institute, a cooperative, educational association at http://www.sans.org/aboutsans.phb as well as various private firms including Verisign (http://www.verisign.com/), Symantec (http://www.symantec.com/index.htm and http://www.enterprisesecurity.symantec.com/SecurityServices/content.cfm?ArticleID=5039), Cisco (http://www.cisco.com/), Counterpane (http://www.counterpane.com/), TrueSecure (http://www.trusecure.com/). For additional information about security advisory industry see http://www.securitypipeline.com/news/49400256

procedures have already been introduced into many firms in the financial sector.[51] Such procedures in the financial sector have, of course, been given impetus by bank supervisory authorities who have a mandate to ensure the safety and soundness of financial institutions. In this way both external and internal pressures have been generated to improve mechanisms for risk assessment and management.

In addition, there are important bodies of international standards that are becoming a reference point for improving cyber security practices. The ISO/IEC 17799 Code of practice for information security management[52] standard (soon replaced by the 2005-version) is a "good practice standard" for the application of information security in public, semi-public, and private sectors. Some multi-nationals require business partners to comply with this standard before they allow electronic access to their services or contract services of such a business partner. See the discussion of supply-chain relationships in Appendix A.

Risk management:
manage threats or outcomes?

One topic that was discussed during the research for the case study was risk management. None of the interviewed firms described their cybersecurity efforts as "risk management", which most thought of as being a more structured activity than what they were doing.

While discussing risk management, more than one security executive said that they doubted that a quantitative risk analysis could be completed due to the unknown (and, according to one executive, unknowable) threats, and probabilities associated with those threats. In the absence of actionable knowledge about threats and probabilities, these security executives adopted an approach where they managed the potential outcomes of imaginable vulnerabilities. This often resulted in the firms deploying redundant systems such as geographically distributed database and email servers, and redundant routers in their internal networks.

Third party firms such as security consultants or potentially insurers are likely to facilitate the flow of experience and expertise on a cross-firm basis. Such flows can be stimulated through formal institutional arrangements and structures such as Information

[51] See the World Bank financial sector study for a detailed discussion of such procedures.

[52] Derived from the earlier BS-7799 standard.

Sharing and Analysis Centers (ISACs)[53] or through similar intra- and inter-sector organizational structures. However, it is important from a practical standpoint to understand how such critical information actually is exchanged among private entities as well as public, semi-public, and private entities. There is no one single model for structuring and handling these information flows. Approaches will differ from firm-to-firm, sector-to-sector, and country-to-country. The complex dynamics of this process are more fully discussed in sections III5 and III6.[54] [55]

Another important factor in reshaping the process of risk management and assessment may be the nature and credibility of intelligence service or law enforcement agency generated information that is provided to senior corporate decision-makers. Such information is likely to influence significantly the entire process of risk assessment and management. This is a delicate and sensitive area of public policy concern. It relates to the protocols and understandings upon which sensitive publicly generated intelligence information may be provided to private sector entities and the conditions on its further use or dissemination. It relates as well to perceptions about the symmetry of information flows from the private sector to the public sector—and vice versa.

[53] An ISAC offers a framework for exchanging information between multiple organizations. ISACs can communicate intra-sector only, can be a private sector ISAC communicating with the public sector (industry with government agencies), or can communicate inter-sector with other ISACs. Until now the ISAC model is mostly used intra-sectors. The U.S. Department of Homeland Security has established ISACs to allow critical infrastructure sectors to share information and work together to help better protect the economy. In Australia they are referred to as Trusted Information Sharing Network and in U.K. they are associated with the Assurance Report Program.

[54] Based upon information collected by Martis, E.R., Luiijf, H.A.M., and Geers, J.M.E., TNO, The Hague, The Netherlands in 2004 for an investigative project on Computer Security Incident Response Teams.

[55] EU Handbook of Legislative Procedures of Computer and Network Misuse (http://www.europa.eu.int/information_society/eeurope/2005/doc/all_about/csirt_handbook_v1.pdf)

Ultimately, there is an impact on the trust relationships that are established between the public, semi-public, and private sectors as it relates to the performance and effectiveness of risk assessment and management in the private sector.

There is one point of over-riding and strategic importance. Effective cyber security policies will depend on strengthening and reinforcing the mechanisms of risk assessment and management at the enterprise level, either of a company, an organization, or government department or agency. This process will require more focus on how corporate risk management can be more “outward-orientated”. This means increasing flows of security-related information among the various key business and sector-related relationships of an enterprise. It is also likely to require better collaboration and timely communications with public agencies concerned with cyber security policy. However, they are often unable to provide information on a timely basis and in such a way that can be acted upon. Public agencies often need to significantly sanitize information leaving threat information vague and unspecific. [56]

The bedrock of cyber security policy will be “bottom up” initiatives. Policy-makers will need to give increased priority to assessing ways that public officials can support and energize increasingly effective ICT corporate risk management rather than “drive” policy and risk management programs on a top-down basis. This creates, however, the need for a basic model or models for sharing information from sector to public agencies and vice-versa. One approach may be to start with a limited or small-scale environment and “light-weight” threat information exchange scheme based upon a well-designed, scaleable, and thorough scheme or standards. Using such a scheme on a national, regional, or international basis, it might be easier to interconnect ISACs and

[56] In some case, the information may be so vague and unspecific as to be of limited use. Consider the following hypothetical communiqué: “In the next six weeks there is a high probability that someone, probably on the northern hemisphere, may target a computer centre”.

public, semi-public, and private sectors if and as the need to do so arises. The outlines of such an approach are described in further detail in Part V.

It will be difficult, however, but very important, to reverse policy predilections to direct and coordinate concerns about security policy from the top down—from agencies with historic and longstanding responsibilities to protect vital interests of the nation state. In the absence of top-down policy, what are the incentives and drivers that will affect an increase in the level of information security to what is needed to protect critical infrastructure?

As noted above in Section II.1, there are already forces in place that act to bring about much of the desired improvement in information security that might be desired by public officials; the root issue was in how public and private entities went about defining an "adequate" level of information security. What does it mean for a firm or other entity to have an "adequate" level of information security? For what is this level of information security adequate? A rational approach to defining 'adequate' involves managing the entity's risk by looking at the vulnerabilities, probabilities of successful exploitation of those vulnerabilities, and outcomes if those vulnerabilities are exploited. The incentives for security arise from the expected costs that are uncovered. Few security managers explicitly adopt this approach, instead relying on their experiences and received wisdom to guide them in adopting a security posture.

This approach leads to a very "localized" viewpoint of information security. Without the discipline imposed by thinking in terms of risks to the organization, security managers are likely to think in terms of risks to their "local" machines and applications. This internal focus results in a suboptimal security stance for the entity as well as creating externalities that are perceived as market failures.

Relying on past experience and received wisdom also leads to reactive information security, where entities adopt a security measure in response to past attacks or to the latest well-publicized information security phenomenon. Firms that explicitly manage risk are much more likely to ask “what if” questions, and adopt a more customized, robust security stance.

For example, consider the security management of a home computer. The great majority of users are interested in maintaining the usefulness of the home computer for surfing the web, email, word processing and other tasks. From this purely local viewpoint, the incentives for the user to protect their machine are to maintain connectivity, and to protect data they value. If the user does not store valued data on the machine, a user may not adopt any security measures until the machine is infected with a virus that interferes with their use of the machine or causes the user’s friends to complain about the email viruses they are receiving. From the local point of view there is little incentive to invest in security against viruses, trojans, worms or other malware unless it affects the user’s ability to use the machine. Such unprotected machines form the core of botnets used to propagate spam and source ddos attacks[57] which can impact many other users.

Contrast this with the security manager of a financial firm. Her focus is not only or even primarily on her local machines being free of viruses and worms; it is also on assuring the availability of her firm’s services and on the integrity and security of data as it is being held internally and passed, for example, between her firm and other financial institutions and customers. She has a much broader view of what is being protected: her customer’s data and data networks as well as her local machines and data. Consequently, she invests in information security at a level consistent with this definition. Her incentives are quite different than the user in the example above: she not only needs to protect her client’s data (money) internally, but she also needs to assure client’s data is protected by her business partners, and be regarded as a secure entity by other financial institutions so that her firm can operate effectively. It is likely she explicitly manages risk as described above.

[57] John Leydon , Oct 20 2004 http://www.theregister.co.uk/2004/10/20/phishing_botnet/

Most firm’s definitions of what is being protected lies between these two extremes. Even within a given business sector or sub-sector, firms will take a variety of views as to what they are protecting, with some firms adopting very local viewpoints and others adopting more inclusive definitions incorporating interactions with other organizations. We believe that absent external forces such as regulation, the relative information security stance assumed by an organization is correlated with the inclusiveness of what is being protected. For example, within a particular industry some firms will think that protecting their local machines, applications and data is adequate. Other firms in this industry will feel they need to assure the security of their communications and data transactions with members of their extended enterprise, and adopt a more sector-level view of what needs to be protected. Graphically, this is expressed in panel ‘a’ of Figure 1, where the level of security is higher when a sector security good is addressed rather than a purely local security.

External forces such as regulation will affect this correlation. If we return to our financial sector example, the plot would look as is shown in the ‘b’ panel of Figure 1. In this case, the level of the local good is the same as the level representing the sector good. This is a result of the regulation imposed on the industry as well as network effects: if financial institution A’s security is not adequate, then other financial institutions will not conduct business with A. In this case, the minimum acceptable level of security is that which also meets a sector good.

Thus, a key to promoting more effective information security, not just in firms but in all entities, is to encourage them to take a much broader view of what they are trying to protect. One concrete step towards this goal is discussed above: getting corporate boards to view information security as a board-level responsibility. Corporate boards by their very nature take a very broad view of firms activities, and are strongly predisposed to not think in local terms regarding security, particularly if cyber security awareness-raising activities are effective. While few boards are expert in cyber security matters, they have

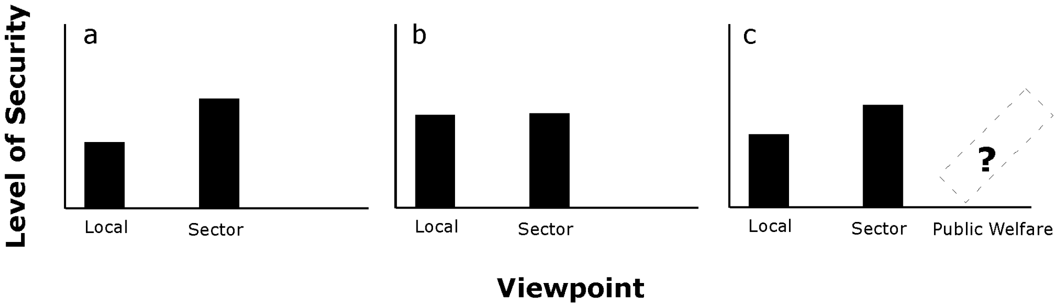


Figure 1. The levels of information security adopted when using a strictly local (e.g. internal to firm) and a broader (sector) point of view. In some business sectors a broader view will result in greater security, as shown in panel a). Other sectors that are heavily regulated or require tight integration between individual firms (such as the financial sector) are likely at the point that the appropriate level of security from a local view is the same as from a sector view, as shown in b). Panel c) tries to represent the unknowns of what constitutes an adequate level of security from a public welfare standpoint; the risks that need to be addressed might be completely different than those considered from a business perspective. This is not to say that they are necessarily different: indeed it is likely that they are very similar, and that merely by rationally addressing risk from a broader point of view firms will address most of the risk facing the public welfare. In other words, enabling firms to effectively address their risk will address most of the public risk.

the option of hiring consultants who are, or asking for audits of their firms' compliance with developing standards such as ISO 17799.

Another concrete option for helping security managers at firms think in broader terms is to promote their adoption of the network model at the core of this discussion paper. Through the development of an understanding that they and their firm are playing a role in a highly connected network, they will naturally become aware of the effects they have on others, and the effects that others can have on them. This broadened appreciation of the risks they face will result in a broader view of what they are trying to protect.

Wanting to preserve your firm's ability to operate is, of course, an incentive from a "gain" perspective. There are also incentives resulting from "pain", resulting primarily from the public knowledge of a firm having been the victim of a cyber event that resulted in harm to its customers. While it is seldom in the interest of any firm to publicize such events, firms' suffering as a result of security insufficiencies is part of the creation of an environment where firms take cyber security seriously. This may require a change in public policy.

The Public Welfare: So far we have been looking at security from the firm’s point of view: what a firm might reasonably do in their self-interest. Recall that in the introduction we showed two sources of desire for increased information security: business, and the government. What might constitute an adequate level of information security from the viewpoint of the government, and what relationship does this level of security have with the security level firms might reasonably adopt?

The government is primarily interested in addressing vulnerabilities that would cause a level of harm that does not affect an individual firm, but whose effects would threaten the ability of a whole infrastructure to deliver critical services and goods to the population. The National Infrastructure Advisory Council in the United States, for example, has identified eight infrastructures: power (electric, gas, etc.), water, transportation, communication, financial, manufacturing, emergency services (fire, police, 911), and health care. The government is concerned with device and systemic vulnerabilities that have never been experienced; because of the different nature and low probability of these vulnerabilities, it may be the case that rational firms will never adopt a level of information security that would address these vulnerabilities. Put another way, the types of information security desired by the government may be different than those that individual firms might consider; it is proper to think of the types of information security needed for the public welfare as not necessarily being better, but different. This is represented in panel ‘c’ of Figure 1 by the angled bar.

This is not to say that there is no overlap between a sector’s interests and the government’s interests. It is likely that the financial industry’s interests and the government’s interests are closely aligned. The aim will be different, such as in the case of power sector companies and higher-security SCADA devices: the government would like to see these more secure devices; the companies see no or little economic incentive to upgrade. In the discussion we will address mechanisms that seem to be effective at promoting the adoption of higher security in cases such as these.

Managing Acceptable Risk: As we saw above, the government is looking promote the development of protection against information attacks that have been hypothesized, but have never been seen: the government is trying to manage this risk by proactively reducing these vulnerabilities prior to suffering any consequences. The difficulty is that most firms are averse to investing in security against events that have never occurred, even if they might worry about them. Many firms are similarly reactive in their security investments, responding to actual vulnerabilities. Implicitly, they are not managing risk, but closing known vulnerabilities.

The key question is whether any rational firm would be expected to invest to protect against such risk. To the extent that firm interests and public interests are aligned, and rational firms will invest to reduce risk, then the need for public policy is minimal – perhaps to make markets more transparent, but not any stronger. If it becomes the case that public officials are concerned about a credible threat that firms rationally ignore, then stronger policy measures, such as regulation, may be required.

5. Improvement of information sharing on a formal and informal basis

It is apparent from the foregoing discussion that a careful analysis of flows of information relating to risk management of cyber security concerns—on both a formal and informal basis—is a critical part of any overall program to establish more effective ways to protect critical information infrastructures. Such an analysis cannot be carried out on a formulaic basis. It must take into account substantial differences in public, semi-public, and private structures, governance mechanisms, legal structures, and the level of interaction of all these factors in strategic, tactical, or operational terms. There are also very differing approaches to risk management in the different sectors and in different countries. In the U.S., these differences in approach to risk management are now being explored by a public-private sector working group that will report to the National Infrastructure Advisory Committee (NIAC), a high level private sector advisory group to the Department of Homeland Security.[58] Because of fundamentally differing approaches to risk management, any effort to improve risk management on a comprehensive basis—across a spectrum of sectors and countries in differing stages of development must be empirical and pragmatic. It cannot be effective if based on a "one institutional prescription fits all" approach in terms of any recommendations for organizational or restructuring initiatives.

It is critical to determine how and what types of information flows are involved in risk management schemes and how changes in such flows could influence the effectiveness of risk management initiatives. It is also critical to access not only the formal structures for collaboration but examples of spontaneous and real-life experience with information sharing which can be built upon and made more effective. For this reason, the focus of policy-makers is, or should be, as noted above, on the better delineation of "networks of information flows"—on flows that might today exist or might need to be further developed in the future. Policy-makers may also find it useful to give priority to tools and mechanisms such as exercises that may facilitate better understanding of, and improvements in, information flows critical to dealing with cyber threats and incidents.

We discuss below in Part III the various ways that such information networks can be described and viewed by policy-makers and other participants in such information flows. Such networks can be viewed from the vantage point of the various participants in the process. The differences of perspective relating to the risk management process—depending on the point of view of each "information network participant"—may be important to make more explicit and "visible" to the entirety of those who participate in a set of "networked relationships" established to deal with cyber security concerns. As noted above, the NIAC Working Group was established in the U.S. to understand the

[58] For background on NIAC see http://www.dhs.gov/dhspublic/display?theme=9&content=3445

different approaches to, and expectations about risk management by the public, semi-public, and private sector participants.[59] This "network model" is described in further detail in Part III below.

6. Development of mechanisms to respond to cyber incidents

One of the most critical aspects of an overall cyber security program is the capability to detect, to investigate and analyze, and to respond to cyber-related incidents. Various organizational forms have been developed at a multitude of organizational levels (ISP, enterprise, intra-enterprises, intra-universities, sector, national, and international) to investigate, analyze, and respond to cyber security incidents. Many of these organizational structures have been developed bottom-up by professionals based on conviction that effective security depends on shared responsibility. During the last years, attempts have been made to establish similar organizations on a top-down basis; however, these efforts have not generally been successful.

As noted above, the so-called Computer Security Incident Response Team organizations or CSIRTs[60] have very different forms because of the differences in their set of tasks and responsibilities, constituencies, and scale of operations. These differences are described in detail in Appendix B. A special form of CSIRT is an Information Sharing and Analysis Center, which acts as an independent commonly-funded clearing house for information-sharing between "connected partners". The ISAC offers sanitized and anonymous information on threats, sector-specific vulnerabilities, and incidents, as well as threat, incident, and trend analysis capability.

The main aspects related to the establishment of CSIRTs and their relationships with other computer security incident response mechanisms are:

[59] Background information on this Risk Management Working Group as well as information on other analyses undertaken by NIAC relating vulnerabilities and cascading risks can be found at http://www.dhs.gov/dhspublic/display?theme=9&content=3445

[60] Note: the term CSIRTs comprises the term Computer Emergency Response Teams (CERTs).

- What constituency is the CSIRT responsible for?
- What organizational level of responsibility do they have? What is their mandate arising from the enterprise, set of organizations, nation they serve?
- Does the CSIRT meet a minimum set of quality standards (e.g., accessibility on a 24*7 basis via multiple media, trustworthiness, documented procedures)?
- What national and international ***trust-based*** relationships have they established and do they maintain with other computer security incident response organizations? Are they part of one or more "webs-of-trust"? It should be noted that without trust, CSIRTs are hampered in exchanging and sharing information about vulnerabilities and sensitive incidents. There are some developing standards, e.g. Trusted-Introducer, in this area (see Appendix B for further details).
- Does the CSIRT link into higher levels of computer security incident response capabilities, e.g. to regional or international coordinating CERTs and organizations, like CERT/CC and FIRST?
- Depending upon their responsibility and national/ regional/ international tasks, which relationship has the CSIRT established with justice and law enforcement agencies? To media? To national intelligence and security services?

ISACs have the additional problem that they connect in their "constituent group" a set of private organizations which have competing goals, but commonly need to provide the ISAC with incident information which can analyzed, and disseminated and shared by the ISAC in an anonymous and sanitized way. The ISAC needs to deal with the sensitivity of commercial information on the one hand, and the importance of fast reaction with as detailed information as possible to prevent cyber security events from creating trouble on a sector-wide basis. At the same time, government agencies may want to require such data for their own watch and warning processes, while often having problems in sharing with the ISAC and its associated industry sector their own relevant analyzed information about threats to the sector. The bi-directional flow of information sharing is, however, crucial for effectiveness of addressing the joint problem of cyber security and the ability to identify malevolent actors.

Unlike formal ISACs, informal ISAC-type organizations, e.g., BITS[61], operate through high-level informal ties at a senior executive level in the financial services sector as well in other sectors in various nations. Various advisory firms as well as software and hardware suppliers can also act as an effective conduit for information among firms in the same or related industry sectors. As is emphasized in World Bank studies of cyber security arrangements in the financial sector, effective intra-corporate arrangements and procedures for responding to cyber incidents are one of the key elements of a well designed set of ICT corporate governance arrangements. Thus, any initiatives to develop new or enhance existing CSIRT-organizations and capabilities at sector-level will need to focus special attention on the integration of CSIRTs into incident-related flows of information within firms, from individual firms to related firms in the same sector, and from these firms to firms in other sectors. Above all, such initiatives should take into account the issue of trust and willingness to effectively share incident-related information.

Likewise, it is likely to be important that collaboration among CSIRTs at the national level not be hierarchical. There are likely to be significant peer-to-peer flows of information, especially within multi-national firms, but also within specific CSIRT bodies that might deal with cyber-related incidents on a cross-border basis.

It is too simplistic a policy prescription to focus on creating new or enhancing existing CSIRT or ISACs organizational structures at the national level without concurrently developing an entire capillary structure for information to flow into and out

[61] For background information about BITS see http://www.bitsinfo.org/ and its initiatives in the security area (http://www.bitsinfo.org/secrelini.html)

of, and among, firms and government agencies in critical infrastructure sectors. There is a dynamic, organic network building process for such incident prevention, analysis, and response capabilities. This process mirrors the networking dynamics of the new IP-based information and communication technologies as opposed to the more structured, hierarchical nature of conventional telephone networking.

Another key piece of the overall institutional architecture is how industry-oriented CSIRT procedures are meshed through government-directed coordinating entities[62]. It is also important to assess how cross-border flows of threat information are managed, tracked, and overseen. Equally significant is how the overall coordinating structures for critical information infrastructure protection are meshed with mechanisms for dealing with risk management with respect to communications infrastructures like the Internet, which may be overseen by telecom regulators or ICT ministries. We turn next to this issue.

7. Improvement of regulatory tools and mechanisms for minimizing risk to telecommunications including the Internet-related infrastructure

In a number of countries including the United States with its longstanding and well-developed regulatory infrastructure, there are well-established regulatory mechanisms for dealing with emergency or crisis management scenarios. For many regulators in countries where independent regulators have only recently been established, the experience of the U.S. may be illustrative of the potential role of regulators in establishing an industry forum to identify "good practices" for dealing with new cyber-related risk.

[62] The CERT CC organization maintains ties with a wide range of private sector organizations including ISACS, individual firms, and other sector specific organizations. There is considerable speculation about the ease with which information from individual firms that might be sensitive from a commercial standpoint is shared with CERT CC. The fact of the matter is that the relationships among CERTs and private sector participants cannot be characterized in simplistic, organizational terms.

The U.S. Federal Communications Commission is involved in dealing with cyber security issues through the National Reliability and Inter-operability Council (NRIC), a long established organization that has been re-chartered in recent years to deal with cyber security issues. [63] The NRIC is effectively an FCC advisory committee in which FCC commissioners (usually the Chairman and another member of the FCC) participate working through various advisory committees of senior executives as well as working group experts. The NRIC currently works through a number of working groups. The NRIC does not promulgate or propose recommendations or regulations to be adopted by the FCC. It focuses on developing best practice documents and increasing awareness of these best practices within an increasingly diverse industry structure. [64] These industry outreach efforts are of critical importance. The structure consists of industry arrangements and multiple industry players including fiber backbone providers and ISPs. Many of the NRIC's recommendations and best practices may provide useful guidance and approaches for service providers of backbone infrastructure and ISP services.

What is significant as well about the NRIC approach is its flexibility in the face of the emergence of new mobile services and new network architectures including what is often referred to as Next Generation Networks (NGNs). The increasing speed of implementation of mobile and wireless LAN networks has created potential new security-related challenges and vulnerabilities for established wire-based network infrastructures to which new network technologies are being attached. Best practices developed to deal with these challenges are likely to have significant relevance to regulators and industry players in other countries. One of the important challenges facing executives and regulators involved in the NRIC process is how to make its work more universally accessible and responsive to service providers and regulators in other countries.

For example, in the U.S., the coordination of the national telecom infrastructure in times of national emergency is handled by the National Communications System.[65] The National Coordinating Center for Telecommunications (NCC) has been established as an ISAC for the telecom and information sector. The National Security Telecommunications Advisory Committee (NSTAC) consists of a high level board of CEOs from the telecom sector, hardware and software manufacturers, information and system security providers, major information users, and trade associations whose members are directly appointed by the President of the United States.[66] NSTAC members often receive classified intelligence briefings—a practice which is not representative of current practice relating to flow of classified intelligence information to private sector executives in critical information infrastructure sectors generally.

[63] http://www.nric.org/

[64] A guide to NRIC best practices can be found at http://www.bell-labs.com/cgi-user/krauscher/bestp.pl . NRIC operates through a series of focus groups that are described at http://www.nric.org/fg/index.html

[65] For background on the National Communications System, see http://www.ncs.gov/about.html

[66] For background information on NSTAC see http://www.ncs.gov/nstac/nstac.html

Harm, Control, and Incentives

Any mechanism that will hope to promote information security must assure that the incentives for improvement are focused on those who are best able to affect greater security.

For example, home users have little initial motivation to secure their machines, as noted above. When their machine is infected with a non-destructive virus, worm or spyware, the user suffers a slow machine; in the case of destructive viruses the pain experienced by the home user is much greater (and will usually result in the user securing their machine using AV software).

Note that home users suffer the harm, but are not in the best position to reduce the risks associated with viruses and worms. OS and application vendors who control the design and implementation of the software, are in the best position but in this case experience little or no harm due to the lack of security of their products. If vendors were liable for the security performance of their products, there would be a strong incentive for them to increase the security of their products. For a longer discussion, see Anderson 2001 (www.acsac.org/2001/papers/110.pdf)

Another significant challenge is how to ensure that officials concerned with the protection of critical information infrastructures understand that rapidly changing technological architectures and new industry structures are very likely to affect the basic security of other critical industry sectors as those are increasingly dependent on ICT. Independent regulators and industry participants in the telecommunications and ICT-sectors with specialized understanding of the emerging security challenges can play a critical role advising the private sector and other public sector agencies on the protection challenges and the need for urgency. They can also have an important role in emerging economies highlighting the potential adverse impact of spam on the basic telecommunication infrastructure and on broader cyber security-related risks that spam can generate. The same is true for the expected next threat of spamming of Voice-over-IP (VOIP) telephony, and Instant Messaging (a.k.a. spimming)

The role of telecom regulators in dealing with spam and cyber-related risk was highlighted at a meeting of the ITU-sponsored Global Symposium of Regulators held in Geneva in December 2004. The potential adverse impact of spam is now becoming very apparent in many emerging markets. Limited international broadband connections as well as domestic Internet connectivity resources are being heavily burdened by spam-related traffic. Scarce and critical Internet resources are being used in a highly inefficient way. Though the perspective of some emerging market regulators is that the problem of spam originates from a limited number of highly developed markets such as the U.S. market, it is also apparent that vulnerable and poorly protected infrastructure in emerging markets can become a breeding ground on a secondary basis for spam attacks domestically and internationally. Zombie code can become embedded in poorly protected networks and PCs in emerging markets. Concerted spam-attacks can create a broader range of security risks through denial-of-service attacks against critical information infrastructure or through cyber crime activities that can have a significant deleterious impact on national economies.

In many emerging markets, where independent regulators are becoming involved with dealing with spam-related concerns, cooperation is beginning to open up and evolve with national CSIRT organizations. In addition, in Nigeria, the Nigerian Communications Commission is a member of an inter-agency group dealing with cyber crime which has the two-fold purpose of dealing with the security of computer systems and networks as well as the protection of the critical ICT infrastructure. See the grey-shaded insert below.[67]

Another avenue for the involvement of telecom regulators in cyber security concerns has been through the International Telecommunications Union (ITU) and its Study Group 17 dealing with cyber security in the ICT sector. The ITU has co-sponsored three recent symposium dealing with cyber-security—one in Florianopolis, Brazil in October 2004, another in Moscow in March 2005, and a third in Riga, Latvia in May 2005. These meetings have been organized in collaboration with other organizations concerned with cyber security. The latter meeting was undertaken in collaboration with the new European cyber security organization , ENISA. The Moscow meeting was organized both with Russian ministry officials, service providers, as well as the Russian

[67] See the presentation of Basil Udotai, Coordinator, Nigerian Cybercrime Working Group (NCWG), Nigerian Cybersecurity Porject: Initiative to Secure the Internet for Economic Development and Growth, Afrinet 2005, Abuja, Nigeria, February 2005

Association for Networks and Services (RANS). RANS has also been active in organizing bilateral consultations relating to cyber security with an Indian counterpart, NASSCOM. For its part, NASSCOM, in collaboration with the Indian Ministry of IT, has been the point of contact for dialogue with IT and software companies in the U.S. concerned about cyber-security aspects of significant outsourcing relationships among U.S. and Indian firms.

Through its efforts, the ITU has been working closely with international IT, telecom infrastructure, and software firms to increase awareness, on a country-by-country and regional basis, of the importance of increased cyber security in the backbone infrastructure. These efforts are relying heavily on multi-constituency industry associations like RANS in Russia and NASSCOM in India to ensure a comprehensive involvement of concerned stakeholders in the telecom sector and beyond.

An important question for policy-makers is whether a bifurcation of responsibilities among telecom regulators and agencies more specifically concerned with cyber security is inevitable or desirable. [68] Where independent regulators do not have a legacy role in dealing with network security issues, it may make more sense to encourage new ways of dealing with backbone security concerns through the webs of CSIRT and ISAC mechanisms described in the sections III5 and III6 above. Interestingly, however,

[68] Nevertheless, in many countries, it would appear that there is a kind of partitioning between the telecom/IT security community and those generally concerned with cyber security. This dichotomy is visible in many different respects—in responsibilities within regional organizations such as the OAS where issues of standardization are deal with through CITEL, a regional collaborative body of regulators but the establishment of CERTs is being driven by the counter-terrorism group in the OAS. Another example of bifurcation of roles and responsibilities between the telecom and security sectors is provided by the U.S. experience. Within the Department of State, relationships at the international level with the ITU are vested in a bureau different from the Department bureau responsible for general security concerns. There exists, as a practical matter, a kind of stove-piping of closely related areas of strategic concern. Telecom-related issues within the purview of the FCC are addressed in a bureaucratic arena that is seemingly partitioned off from the core responsibilities of the Department of Homeland Security. The FCC has long been able to navigate in a grey space between its well established regulatory independence and its critical role working with executive brand agencies on infrastructure security issues.

in Finland, the Finnish CERT, CERT-FI, was established under the umbrella of the Communications Regulatory Authority (FICORA).[69]

Integrating telecom and information infrastructure security concerns with an overall cyber security framework may be a complex task in countries which have only recently established regulatory bodies. These bodies are already faced with a complex array of new challenges including issues of convergence of services and technologies, like SMS integrating with e-mail, Voice-over-IP, and so on. It may be more difficult for "new" agencies with newly minted independent status to achieve credibility in areas of national security policy. Such areas have been the near exclusive domain of ministers of the interior or ministers with defense or intelligence related portfolios.[70] Thus, the challenge facing new regulators or ministers with an e-economy portfolio may be how to establish an overall e-security framework in which basic telecommunication, global grid, and Internet backbone security concerns are only a part of much more complex and inter-related institutional arrangements

Telecommunication regulators or e-economy officials can, however, take a leading role in establishing institutional arrangements in which they may not have the lead role. They can seek to establish a comprehensive and well-ordered set of relationships which address the complex and "networked" nature of emerging cyber security challenges. Such a "catalyst" role is fully in accordance with the broad mandate that is usually part of e-economy minister's task of developing and exploiting the potential impact of ICT-services on a range of public, semi-public, and private sector

[69] Background material provided through the OECD.

[70] Indeed, security of government-related networks is likely to have been within the responsibility of ministries relating to defense or intelligence or at least sections of ministries of communications with a close nexus to these latter agencies. Often, issues of national information security policy, as it relates to economic policy, may have been vested with ministries of economic affairs. In many countries, of course, there may not yet have been established coordinating mechanisms to deal with homeland security or cyber security policy.

activities. Regulatory and e-economy ministry officials can also develop a well-structured approach to ensuring that the new ICT-related risks with a potential impact on other critical information sectors are properly allocated through liability-related legislative, administrative, or contractual measures. They can also play a key role in the enforcement, monitoring, and coordination of national cyber security policies in a domestic and international context.

Such officials can also play a critical role in providing a first line of defense against a range of new threats arising from the misuse through zombie and other Trojan code in poorly protected PCs connected to broadband services. They can do this by encouraging the market, if not in certain circumstances requiring, a “redefinition” of ISP-services to include, on an integrated basis, access as well as cyber security protections for individual users. There is increasing evidence in some markets that ISP providers are regarding anti-virus and other cyber security protections as an integral part of their service offering. Regulators may be able to leverage business practices emerging in the market through “jawboning” and other forms of “soft regulation”. In so doing, regulators can decrease the likelihood that poorly protected powerful PCs with broadband connections can be mobilized and used against CII operations.

8. Devising effective law enforcement tools in response to cyber incidents or attacks

A further critical element of an overall cyber security program is a sound legal framework and effective law enforcement procedures to take action in response to incidents caused by hackers or others with malicious or criminal intent. In many countries, legal frameworks may need to be updated to address damages caused to nonphysical assets or to impose increased penalties to deter cyber crime. Many global and regional organizations including the Council of Europe, G8, OAS are diligently working through organizations of Ministers of Justice and law enforcement to develop common legal frameworks and share expertise.[71] The Council of Europe Convention on Cybercrime[72] dated November 2001 provides participating countries a harmonized legal framework against cyber crime as well as mutual cross-border law enforcement support on a 24*7 basis. Collaborative initiatives are also critical in the area of cyber forensics (inforensics) and criminal investigations in view of the fact that cyber incidents increasingly have a multi-jurisdictional aspect.

A recent prosecution in the U.S. has highlighted the use of zombie code/ roBOT implanting viruses (of which there are now apparently 4000 variations) by a competitor to stage a denial-of-service attack against two competitive firms that would not "play ball with" and collaborate commercially with their competitor/attacker.[73] This assault involved the use of a UK-based firm to disguise and launch the cyber attack and has resulted in active cooperation of high-tech crime units in the U.S. and in the UK. Such a case well illustrates the importance of sharing know-how and experience among the specialized police units that must be deployed to combat cyber crime.

Another investigation of the Hi-Tech Crime Unit in the U.S., the Russian police, the Federal Bureau of Investigation, and private sector security specialists has honed in on the activities of loose collaborative criminal networks, including groups selling tens of thousands of hacked PCs known as (ro)BOT-networks, to other criminal groups to launch denial-of-service attacks. Crime syndicates around the world have been banding together

[71] See http://www.oas.org/main/main.asp?sLang=E&sLink=http://www.oas.org/oaspage/searchform.asp (searching under "cyber security" for relevant OAS documentation

[72] Often referred to as the Cybercrime Convention http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[73] See Wall Street Journal 11/29/04.

in informal alliances to hack into credit card databases, steal on-line banking details, and extort businesses by threatening with denial-of-service attacks.[74]

Nigerian Cybercrime Working Group: an Inter-agency Effort to Deal with Cyber Security

In Nigeria, as a consequence of a Presidential Committee on Cybercrime, the government has created a Nigerian Cybercrime Working Group (NCWG) as an inter-agency body of law enforcement, intelligence, security, and ICT-institutions along with private sector representatives.[75] The NCWG has established a cyber security forum for the financial services sector. It is intended to build consensus among existing agencies and provide expertise to the National Assembly in drafting new computer security legislation. The working group is to lay the groundwork for establishing new institutional capacity in Nigeria as well as for commencing global cybercrime enforcement relations with the Computer Crime and Intellectual Property Section (CCIPS) of the U.S. Department of Justice, National High Tech Crime Center (NHTCC) in the U.K. and the NPA in South Africa. Importantly, the mandate of the working group focuses broadly on increasing the security of systems and networks as well as protection of critical ICT infrastructure in Nigeria.

Dealing with Cyber Crime and Cyber Security in China

There are rising levels of concern about cyber crime in China as the number of PCs connected to the Internet rose to over 36.3 million by July 2004, a 48.3% increase over the previous year.[76] The number of Internet users increased to 87 million and more than 626, 000 web sites had been established in China by July 2004. In turn, crime statistics reported to the Information Security Supervision Bureau of the Ministry of Public Security increased a negligible level in 1999 to over 12, 000 cases in 2003. These trends have led to consideration of new legislation relating to cyber crime in 2004. Various regulations relating to the protection of computer information systems have been promulgated by the State Council of the PRC. In addition, fifteen Chinese provinces have enacted special local regulations relating to cyber security under the authority of regulations adopted by the State Council.

Chinese policy-makers have given primary emphasis to a program of prevention and have initiated a national program to enhance public awareness of cyber crime. Commercial information security products are being evaluated with the results being shared with the public. A five level security model for information systems is being developed. Moreover, the security level of national critical information infrastructure is being evaluated. Reporting mechanisms for cyber crime victims have been established with an online complaint center being established in every city.

[74] See Mosnews.com April 5, 2005, http://www.mosnews.com/news/2005/04/05/compcrime.shtml

[75] The NCWG includes the Nigeria Police Force, the Economic and Financial Crimes Commission; the National Security Adviser, the Nigerian Communications Commission, the National Intelligence Agency, the Nigeria Computer Society, the Nigeria Internet Group, the Internet Service Providers' Association of Nigeria (ISPAN), the National Information Technology Development Agency (NITDA).

[76] See Presentation of Chen Fei Yan, Information Security Supervision Bureau (ISSB), Ministry of Public Security of China, August 2004.

An emergency response mechanism is being set up within the national security community. Telecom companies, ISPs and high-tech companies are being integrated into the response mechanisms. Other measures are being taken as well. Training programs are being established. Private sector research in cyber crime research is being stepped up. Research is being focused in the area of digital forensic technology. Cooperative relationships are being developed with institutes, information technology enterprises, ISPs and other organizations. Priority is being given to establishing cooperation mechanisms in APEC to investigate cyber crimes (in particular, involving child pornography) and to build a cyber crime intelligence database to share information relating to crime trends, digital evidence, digital forensic technology.

The Role of Japanese National Police Force in the Overall Cyber Security Framework in Japan

The Japanese National Police Force has, established a special cyber crime unit that has high tech capabilities to monitor the Internet for evidence of cyber probes that might be the first step toward intrusion of corporate networks and criminal or terrorist activity.[77] It is empowered to conduct security audits of firms. From its law enforcement vantage point, it is taking a leading role on a cross-sector basis in increasing awareness and responsiveness in the business community and among the public to potential cyber risk. It is, thus, very much working on parallel lines with an inter-Ministerial cabinet coordinating committee and programs in individual ministries.

Effective law enforcement tools are one of a set of capabilities that may be utilized in response to computer crime incidents depending on the source and severity of the attack. There is a need for best-practice procedures in cyber incident response and management in public, semi-public, and private sectors, including procedures for seamless involvement of law enforcement capabilities.

There will be, of course, incidents that will originate from organized criminal elements, most of which operate on a cross-border basis. Some of these groups may well be spin offs of rogue elements of former Soviet or Eastern bloc intelligence services that “privatized” themselves as the Soviet block disintegrated and are entirely independent of state control. There may be other situations, however, where autonomous or rogue elements are not discouraged or are tacitly supported by the states in which they operate. Some states may actually encourage such rogue elements as a critical part of their security or military doctrine.

[77] Background information about the approach of the Japanese National Police Agency to cyber security can be found at http://http://www.cyberpolice.go.jp/english/action01_e.html

The only effective way to control such grey area practices is to maintain an effective multi-lateral law enforcement program which supports, if not sometimes tests the credibility of, foreign law enforcement officials in rooting out rogue criminal activity. Credible law enforcement-related techniques can provide for the graduated use of increasingly severe counter-measures against rogue cyber criminals. These could include retaliatory cyber or other measures against a state harboring or supporting cyber criminal activity, and blacklisting financial institutions which are too often involved as intermediaries in money transfers.

9. Development of security doctrine relating to sanctions and response to cyber attacks

As suggested by the foregoing discussion in sections III2 and 0 concerning criminal enforcement and threat assessment, there may be substantial reason to develop and make more public national security doctrines concerning possible circumstances in which overt or covert utilization of cyber defense methods may be required on a retaliatory or pre-emptive basis. There is currently a body of international law including the Geneva Convention that disallows disruptions of critical information infrastructure. Current legal doctrine limits cyber attacks to the military in wartime conditions only where proportionality is guaranteed and the impact on civilians is minimal.

Addressing these questions as part of an overall cyber security policy is not just a matter of theoretical concern. It is a matter of public record that India and Pakistan, Azerbaijan and Armenia, People’s Republic of China and Japan, and other set of countries have experienced series of cyber attacks and counter-attacks at times of increased tension in the relationship between these countries.

The potential challenges for future national security policy regarding cyber attacks with national security impact are likely to be very significant. Evidence of the “source” of an attack may be very difficult to track, especially when the computer resources of third parties can be mobilized by BOTs and directed by an entirely independent, covert hostile party. Tell-tale evidence of a risk of a potential attack—as signaled by a range of probes or intrusions—may not be available to the traditional intelligence or signals intelligence agencies through conventional “interception” and “de-encryption” techniques. Rather evidence of potential probes may be cumulative, develop over a long term period of time and be better collected and assessed by private sector entities closer to a potential point of attack. “Piece parts” of evidence that are available to different industry players may need to be collected and analyzed on a shared basis. Evidence seen at the either the private or government enterprise level may not fit into any pattern or context unless such data is viewed in the light of other appraisals or assessments that might be gathered by intelligence or law enforcement from their own sources or through the combined resources of such agencies in other countries.

In the event of a cyber security-related incident, moreover, the first stages of management of a response, at least until some “triage” judgments about the nature and source of an incident has been completed, are likely to be handled entirely at a enterprise level. Key decisions must be made about how information about a potential threat or incident might be escalated and ultimately brought to the attention of public officials, and/or the public. These decisions need to be undertaken on a carefully calibrated basis and on the basis of agreed protocols among public, semi-public, and private sector officials. It is possible to envision a structured process of transfer of incident-related information through a series of “gates”. The process may not necessarily be on a completely sequential basis. The hand-over or coordination of “command and control” during an incident is likely to depend on its potential severity, sector and (inter)national implications, and practical consequences.

What is described here is a very decentralized model for handling a new range of potential national security threats and for processing risk management-related information relating to critical information infrastructures. Such a model may require significant changes in traditional roles of intelligence and (inter)national security agencies and may require them to operate on a more collaborative, inter-institutional basis than such agencies may have been in the past accustomed to doing.

The real challenge for policy-makers is not just to make adjustment in national and international approaches to information security policy. It is also to establish a new collaborative model for handling a new set of potential national security concerns on an international basis. This may require a complex process of putting in place new procedures and institutional relationships. This is a policy problem that is discussed in further detail in Part IV concerning the role of cyber exercises in developing these new procedures and institutional relationships.

10. Coordination, Command and Control, and Communication in Managing Cyber Security Policies

As suggested by the foregoing discussion, the oversight and direction of an overall cyber security program involves a very complex task of managing a welter of "networked relationships".

- First and foremost, risk management policies must be effectually implemented in CII-related enterprises that are often in either private ownership or autonomous from direct government controls. Lines of communications and collaboration must be effectively structured among all levels of management as well as with counterparts in enterprises in the same or mutually dependent public, semi-public, and private sectors.
- The task of ensuring effective integration of CERT-mechanisms with key industry participants and other governmental entities concerned with cyber security policy is not an easy one at all.
- Ensuring an effective framework for collaboration among regulatory, intelligence, and law enforcement agencies requires an ability to operate at the highest levels of government across a wide range of differing institutional interests. Though there are some market and other institutional forces that are likely to provide impetus to easy flow of information within the CERT-mechanisms described in section III6 above, there are also some significant potential impediments to such information flows. In addition, it is almost a truism

about institutional dynamics and rivalries that differing bureaucratic and institutional interests are likely to hinder or impair the smooth functioning of mechanisms to deal with complex, technologically sophisticated cyber threats, and difficult to trace cyber crime. Thus, it is likely that any effective oversight, or (inter)national coordinating mechanism, to monitor the functioning of the type of "networked relationships" described herein will require the involvement of officials and institutions with high degrees of credibility, sensitivity relating to public-private sector collaboration, and overall influence.

- The coordination task is thus an extraordinarily difficult one and is likely to require a high-level mandate at, for instance, the cabinet or a presidential level as is the case with the National Infrastructure Security Co-ordination Centre (NISCC) in the UK[78] or the U.S. Department of Homeland Security. It may not be possible to accomplish carrying out such a mandate when embedded in a peer level agency, even one with a mandate to coordinate policy, though clearly the nature of any required coordination mechanism will depend on government structure, traditions, and practices.
- It requires as well the ability to deal with intelligence and national defense-related entities on a position of parity as well as to lead and mobilize a complex multi-tiered process of international collaboration. There will, of course, be differing roles and responsibilities for stakeholder institutions depending on whether it is the strategic, tactical, or operational levels of cyber security concerns that need to be addressed.
- It is also essential that the overall cyber security arrangements to be "audited" and monitored on a ongoing basis to ensure that information is flowing over the

[78] The role and functions of the NISCC can be found at http://www.niscc.gov.uk/niscc/index-en.html

various "nodes" in the networked model described herein and that barriers and blockages are not impeding such flows.

Among the core coordinating tasks is establishing the right "neural paths" in the networked model. This is especially important in the international arena where collaborative relationships are sometimes yet to be fully developed. There are also important flows of know-how and experience that must be transferred on an ongoing basis. This may require the utilization of new types of electronic and Internet-related media for training, sharing, and knowledge management of relevant experience. It also requires intensive review of models and modes of trusted communications of incident-related and other information through the networked structure. Effective contingency planning is required to ensure that the integrity of the overall cyber response system can be maintained in the face of any incident that might damage or immobilize conventional lines of communications, both currently and in the future VOIP-realm.

11. Improved quality of system and application software

One of the weaknesses of the current ICT-revolution is the increasing dependency on products produced by a limited number of manufacturers. As is the case with biological system, the less diversity, the higher the risk of a security incident which may have a catastrophic impact on the availability of critical information infrastructures. Any vulnerability in software delivered by market leaders like Microsoft in operating systems for the desktop market (estimated to be at 90%), Cisco in the router market (estimated to have a 70% share), Oracle (41% market share),[79] and other manufacturers in specific ICT-markets may result in such risk. Such 'common' vulnerabilities are exploited by new viruses, worms, and by stealth code imported from websites causing either direct havoc or the establishment of (ro)BOT-networks.

[79] Source of 2004/2005 figures: IDC.

An example of direct havoc is the Sapphire worm a.k.a. Slammer which was released on the Internet around 05:30 UTC on Saturday, January 25, 2003. The spreading doubled in size every 8.5 seconds. It infected more than 90 percent of vulnerable hosts (Microsoft's SQL Server or MSDE 2000) on earth within 10 minutes and caused bandwidth problems in many networks, slowed down responses considerably, and caused, among other disruptive effects, cancellation of airline flights, interference with elections, and ATM failures.[80]

Most of these vulnerabilities can be classified as caused by software development quality problems (e.g., buffer overflows) and default configurations which have too [liberate][confirm] parameter values. For manufacturers with a dominant market share this should create a high responsibility for delivering high quality software. However, common practice is that such software is distributed to the market with a large set of known vulnerabilities due to the lack of product liability of manufacturers for defective software.

Pressure is increasing upon software and key critical infrastructure component manufacturers to change their software and systems which are locked and secured when coming out-of-the-box rather than the current open systems which require awareness, knowledge and a lot of manual actions to secure them. Governments, as main buyers of ICT-products, may develop procurement policies that require manufacturers to deliver secure out-of-the-box software and systems. They also may change legislation to not allow any exemption of software product liability, thus increasing pressure upon software manufacturers to deliver good quality products.

[80] The Sapphire worm has been documented in detail by N. Weaver at http://www.cs.berkeley.edu/~nweaver/sapphire.

12. Building New International Lines of Cooperation and Collaboration

It is almost conventional wisdom that the focus of cyber security policies has, in many countries, been significantly more domestically oriented than is likely to be necessary in the future.

Many senior international policy-makers with long experience and substantial credibility are convinced that a new multi-tiered international framework to deal with future cyber threats needs to be established. This effort would mirror in important respects international collaborative arrangements among intelligence and national security agencies put in place in the context of the Cold War. However, the challenges in responding to a new generation of cyber risks are more complex and require novel cross-border cooperation not only involving governments but private sector entities as well. ISACs and the larger[81] CSIRT-organizations around the globe will, as noted above, need to share more information about threats and vulnerabilities and improve their capabilities based on exchange of "good practices" and experience derived from the operation of different organizations around the world.

Information about cyber threats flows relatively easily within global corporate structures and within globally integrated industry sectors like the financial services sectors, but requires a harmonized interface with other organizational networks of organizations across the globe. Software and hardware suppliers—and a growing number of specialized firms with expertise in cyber security—also contribute to an increased level of shared experience and experience. These information flows need to be better connected into new or just emerging public entities as well as private sector-based ISACs/CSIRTs dealing with cyber security concerns in many countries around the world.

[81] See discussion on types of CSIRTs/CERTs in section III6.

Future policy frameworks will have to take better account of the fact that there are significant differences from country to country and between different sectors in the mechanisms for risk management. These differences reflect wide disparities in corporate governance arrangements and risk management perspectives as well as the supervisory and control relationships among the public, semi-public, and private sectors. Risk management techniques differ significantly within sectors. (Risk management perspectives between the public and private sectors in any one country can differ significantly as noted elsewhere.)

Moreover, there are also very significant differences in how sensitive national security-related policy concerns are addressed and communicated around the world. These differing arrangements around the world are only now being documented; and considerable more work in this area will be required in order to raise the level and effectiveness of international cooperation in the cyber security field.

These differences in national institutional arrangements and approaches mean that substantial time and attention will have to be devoted to weaving new collaborative relationships. These relationships will not fall into place overnight; they will not necessarily negotiated by national leaders and diplomats through new protocols of cooperation. Moreover, they often require the establishment of trust-relationships which inherently is a slow process. New ties and patterns of cooperation will evolve in some cases out of efforts to cope with new challenges – with incidents which require new levels of information exchange and openness. In the complex network model described in this discussion paper for managing cyber security issues at the national level, international cooperation may often be catalyzed through many different participants and at different levels. Integrated globally-oriented companies are in a good position to influence the governments they have to deal with to adopt a more common approach to cyber security policy.

One of the significant challenges for policy-makers may be to explore how joint “exercises” can be utilized in creative ways to create new paths for cooperation and information flow. The discussion in Part IV explores the contribution that cooperative exercises can make to establishing a new structure of international cooperation.

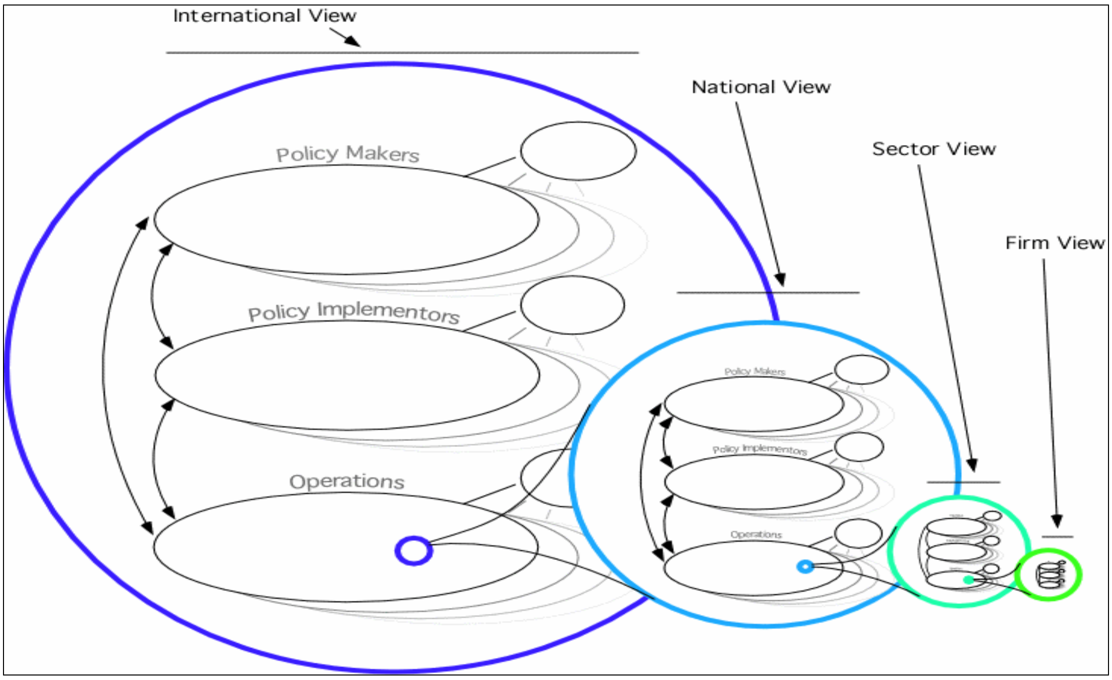
IV A Different Angle of Vision on the Cyber Security "Network Model": Key Nodes and Information Flows

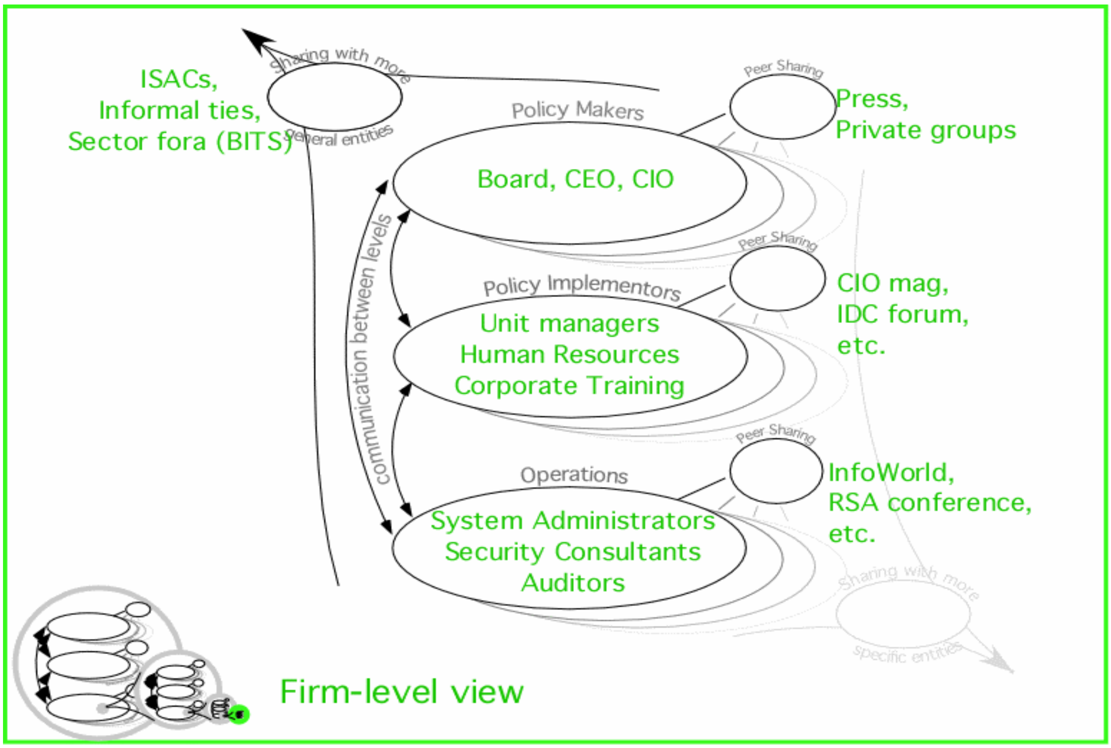
Next we examine the "network model" described herein from a different angle of vision.

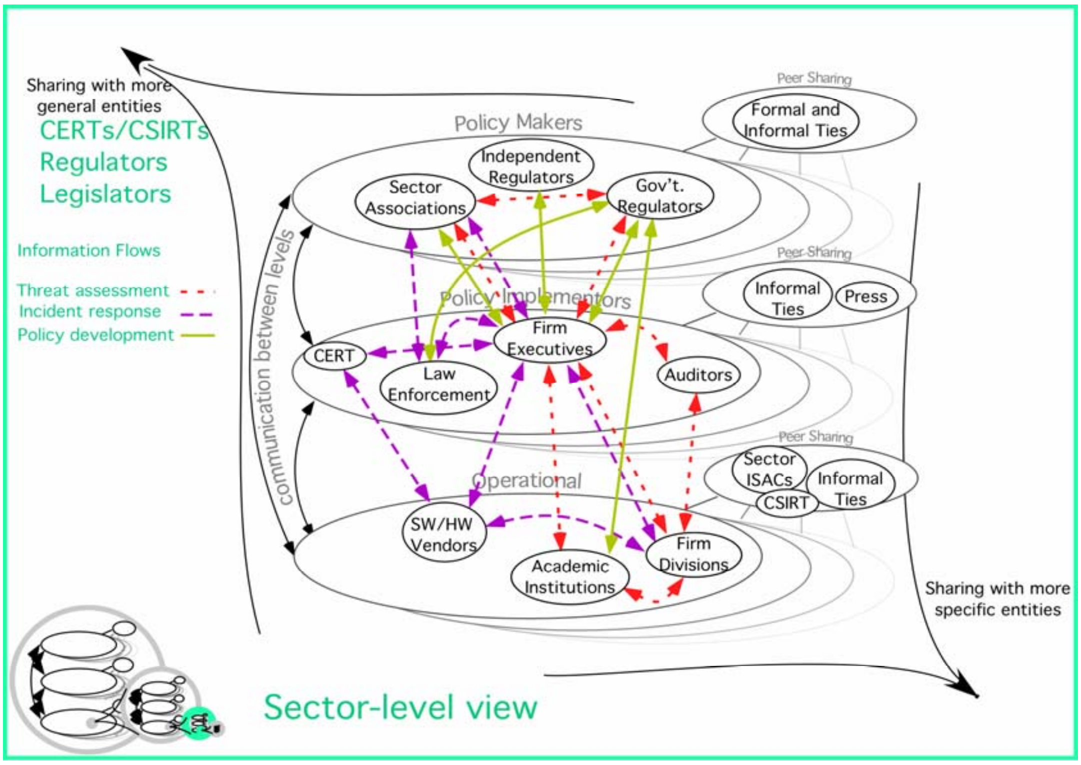
Our focus shifts from the key elements or policy objectives of a cyber security framework to a description and assessment of the key "nodes" and "information flows" in a cyber security "network model". This network model is, as a practical matter, the equivalent of a real communications network. It links different public sector agencies together with semi-public and private sector entities both domestically and internationally over a labyrinth of different communications paths – each related to the various different key elements of the cyber security framework described in Part II. The discussion below focuses on incentives for, and barriers to, these multitudes of information flows.

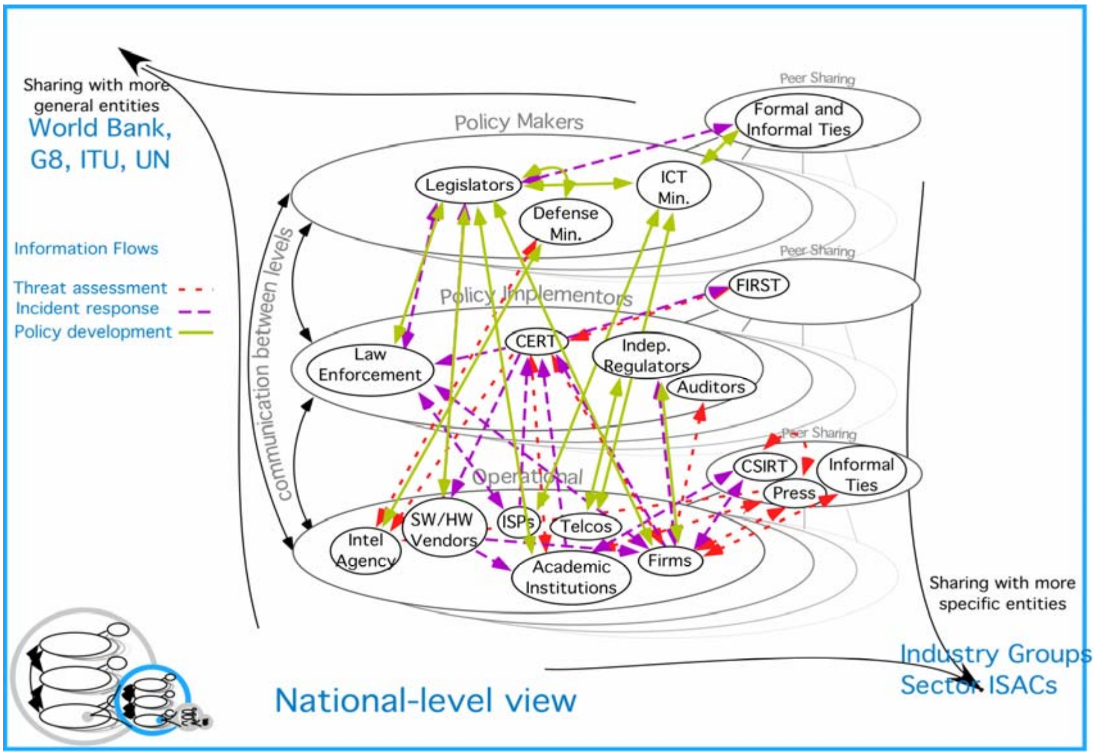
The following diagrams are a visualization of this model which illustrates key institutional relationships. It also illustrates the flows of different types of information that are described in Part II hereof.

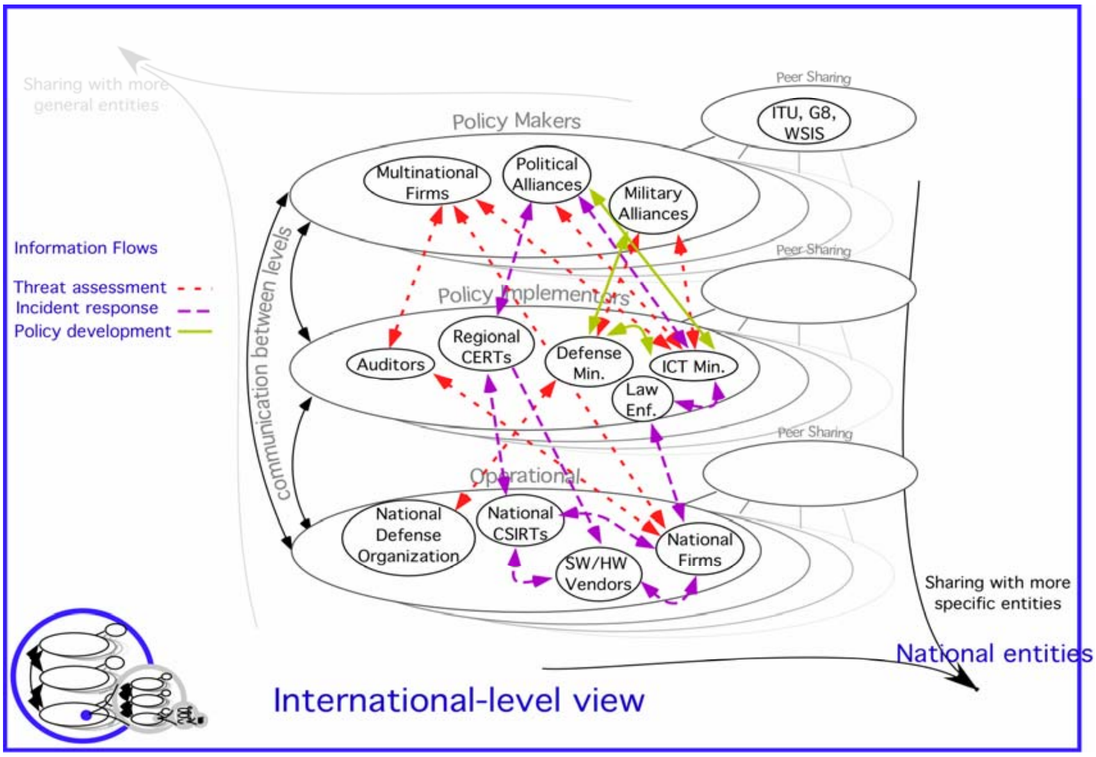
Overview of Multi-layered Aspect of Cyber Security Networks






Sharing with more general entities
CERTs/CSIRTs
Regulators
Legislators
Information Flows
Threat assessment
Incident response
Policy development
communication between levels
Policy Makers
Independent Regulators
Sector Associations
Gov't. Regulators
Peer Sharing
Formal and Informal Ties
Policy Implementors
Firm Executives
CERT
Law Enforcement
Auditors
Peer Sharing
Informal Ties
Press
Operational
SW/HW Vendors
Academic Institutions
Firm Divisions
Peer Sharing
Sector ISACs
CSIRT
Informal Ties
Sharing with more specific entities
Sector-level view


Sharing with more general entities
World Bank, G8, ITU, UN
Information Flows
Threat assessment
Incident response
Policy development
communication between levels
Policy Makers
Legislators
ICT Min.
Defense Min.
Peer Sharing
Formal and Informal Ties
Policy Implementors
Law Enforcement
CERT
Indep. Regulators
Auditors
Peer Sharing
FIRST
Operational
Intel Agency
SW/HW Vendors
ISPs
Telcos
Academic Institutions
Firms
Peer Sharing
CSIRT
Press
Informal Ties
Sharing with more specific entities
Industry Groups
Sector ISACs
National-level view



Set forth below is a brief discussion of key nodes of this model and information flows relevant to these nodes.

Lexicon of Key Parameters of Cyber Security Networks

In this discussion paper we have introduced the concept of a "network model" for viewing the various inter-relationships of key stakeholders involved in a cyber security framework. This network model is also represented in various visualizations included in Boxes 2-6. Set forth below are some of the key parameters of cyber networks:

Nodes: Entities that are involved in carrying out the various key elements or *functions* of a cyber security framework as described in Part II of this paper. These nodes include various governmental bodies such as telecom regulators, IT ministries, intelligence agencies, national security agencies, security policy coordination bodies, various ministries involved in critical industry sectors, finance or economic ministries, law enforcement agencies as well as *private or semi-private agencies* including CERTs, ISACs, special industry groups, vendors, service providers, firms in a range of critical industry sectors including telecom, energy, finance, water, health, food, etc.
Information Flows: The sharing of information among network *nodes* related to functional areas involved in a cyber security framework. Information flows may be bilateral. The information shared in these flows is dependent on the function-specific responsibilities of the various nodes.

Obligations and Expectations: The functions described above create implicit or explicit obligations and expectations between stakeholders in the constituent network *nodes* , which are connected by *information flows*. These relationships can be structured by contract, formal or informal agreements, or administrative procedures or requirements. These relationships can be used as a mechanism for imposing responsibilities or holding counterparts accountable for the activities of networked relationships that are within the span of control of the parties to a paired relationship.

Functions: Each of the key elements in a cyber security framework is realized through the collaboration of various nodes in the performance of a function, such as threat assessment. These nodes collaborate in the performance of a function via the sharing of information with other nodes associated with the function.

Processes and Procedures: The component parts of a function. The nodes and information flows associated with a particular process or procedure are a subset of those needed for the function. As an example, the process of estimating the probability of various attacks is one part of the threat assessment function.

Drivers: These are the mechanisms such as regulatory requirements, the allocation of liability, market signals or information flows (in the case of risk-related information through which the performance of a network may be influenced). Each national networked relationship may operate with its own unique set of additional drivers. Policymakers may shape and structure certain drivers of a network relationship to influence its behavior and performance. It may be possible, for example, to strengthen the influence of market-related drivers by using government procurement policies; liability strategies may result in security rating services or insurance schemes, influencing the cost of access to capital or the incentives to make security-related expenditures.

Inter-operability: The set of *processes and procedures* through which different national cyber security framework can interact with each other. Inter-operability implies that stakeholders in each national cyber scheme understand how to communicate with each other to carry out key elements of a cross-border framework; this is a critical policy concern since it is likely that the *Environmental and Structural Factors* specific to each country result in substantially different architectures and performance of national networks.

Mapping: The process of translating the actual processes and practices for dealing with cyber security concerns into a set of nodes, node functions and processes and information flows in a graphical representation or other structured format. While the exact representation of the cyber security network architecture will likely be unique for each country, identification of the nodes responsible for key cyber security functions across countries will indicate what information flows need to exist between countries in order for those countries to have inter-operable national cyber security networks.

Minimum Levels of Cyber Protection: The minimum cluster of processes and procedures to ensure that a country can participate on a secure basis in the global network. We suggest every country adopt the OECD Guidelines for the Security of Information Systems and Networks: These minimum requirements might be developed utilizing as a reference point or benchmark the OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.

Environmental and Structural Factors Affecting Cyber Networks: A number of factors will influence the overall architecture and functioning of cyber networks including (1) the overall state of IT development in a country, (2) the infusion of IT into critical information infrastructure, (3) the overall state of economic development, (4) the profile of security risks facing each country, (5) the overall legal and institutional framework, (6) the status of any transition toward open and transparent institutions, (7) industry structures, (8) corporate governance practices, and (9)competition conditions.

Network-related Recommendations: In Part V of this discussion paper we discuss certain recommendations relating to the structuring of cyber networks, their *inter-operability* across national boundaries, their analysis and assessment as well as a series of recommended ways for policy makers to view cyber networks.

1. Coordination among Public Sector Entities Concerned with Cyber Security

The following discussions focuses first on a number of key nodes in cyber security networks and their inter-relationships including the roles of (1) central coordination entities, (2) independent telecom regulator and e-economy ministries, (3) intelligence agencies, (4) law enforcement entities and (5) national/government CERTs, and ISACs.

Cyber Security Framework in Brazil: An Important Benchmark and Illustration of the Complexity of "Cyber Security Networks"

Brazil has a complex and very sophisticated infrastructure of institutions involved in developing cyber security policy. Its experience illustrates very well the involvement of many public and private stakeholders—and the role of a web of networked relationships-- that are an essential part of an effective cyber security framework. Brazil provides an important benchmark for other countries developing a comprehensive approach to cyber security.

Information security issues in Brazil are within the jurisdiction of the Institutional Security Cabinet or GSI (Gabinete de Segurança Institucional) (http://www.presidencia.gov.br/gsi/), which is linked directly with President of the Brazilian Republic. GSI is also responsible for other issues such as crisis management, President's security, intelligence, and assistance for President in military and security issues. GSI activities (including information security) are defined by legislation (Decree Nº 5.083, May 17, 2004). GSI does not handle directly security issues, but works through other related organizations such as CTIR-GOV and CGSI.

CTIR-GOV (Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal)(www.ctir.gov.br) is a newly created body with responsibility to handle the national security incidents involving the Brazilian federal government. CGSI (Comitê Gestor de Segurança da Informação) is an information security steering committee (http://www.presidencia.gov.br/gsi/cgsi/)created by Decree Nº 3505, June 13, 2000. It has representatives from every ministry (justice, defense, health, communication, science and technology, etc). The participants discuss information security issues and through working groups define future policy directions of the Brazilian federal administration. CGSI oversees the federal government's commitment under Decree Nº 3505, June 13, 2000 to have an information security policy for every department of the Brazilian federal government.

There are also Computer Security Incident Response Teams (CSIRTs) that have been established in a number of Brazilian states. [Add reference or link to these sites]

One of the important issues under discussion are the mechanisms for achieving cooperation between the Brazilian government and the private sector. Initial steps have been taken to address cyber security issues facing the Brazilian telecom sector infrastructure through cooperation with the Brazilian telecom regulator, ANATEL.

CERT.br, formerly known as NBSO/Brazilian CERT (http://www.nbso.nic.br/index-en.html), is the Brazilian Computer Emergency Response Team, sponsored by the Brazilian Internet Steering Committee and is responsible for receiving, reviewing, and responding to computer security incident reports and activity related to networks connected to the Brazilian Internet. The CAIS (Security Incident Response Team)(http://www.rnp.br/en/cais/index.html) acts in the detection, solution and prevention of security incidents in the Brazilian academic network, besides creating, promoting and spreading security practices in networks. Information about Brazilian Honeypots Alliance with its Distributed Honeypots Project can be accessed in http://www.honeypots-alliance.org.br/ (English).

A number of methodologies for dealing with Critical Information Infrastructure Protection have been developed. Among these methodologies are (1)methodology for identifying critical infrastructures (critical services are identified and ranked according to importance with regard to Brazilian characteristics), (2) methodology for threat identification and analysis (a tool to identify the threats to the critical assets identified), (3)methodology for creating the ideal security scenario for critical infrastructure, (4) methodology to analyze the gap between the ideal protection scenario and the actual one as a means of developing strategies to protect critical infrastructure.

These methodologies have been applied to the Brazilian telecommunication infrastructure. This work has been undertaken with the cooperation of the Brazilian national telecom regulatory, ANATEL. ANATEL is actively involved in the cyber security-related work of the ITU.

Besides Decree N° 3505, there are no specific laws for information security issues. This decree establishes the information security policy in all the government and related partners in a number of different areas including (1)classification and treatment of information , (2) research in technologies to support national defense, (3) accreditation and certification of products and services, (4) assurance of inter-operability of systems, (5) establishing rules and standards relating to cryptography, (6) systems for the confidentiality, availability, and integrity of information, The degree established a center of research and development to security in communications (CEPESC – www.cepesc.gov.br) that will assist and support the executive secretary of national defense, in all aspects related to the information security (scientific and technologic).

There is another law related to defensive electronic war policy, defined by Brazilian Ministry of Defense: http://www.defesanet.com.br/abge/mindefge/. It was published in Union Official Diary n° 59 – Section 1, March 26, 2004.

2. Central Coordination Entities: Managing "Outreach" and the Labyrinth of Information Flows

In a complex, decentralized set of arrangements for dealing with cyber security concerns, there is a critical need for a single focal point or other coordination mechanism to ensure the overall effectiveness and efficiency of the cyber security framework. One of the key roles of such an entity is outreach to the various other national and international public, semi-public, and private sector entities that may be required to collaborate together.

The corporate sector, small and medium enterprises, and the public at large need to be convinced about attaching high priority to cyber security concerns. Senior officials must make the case that new threats and risks relating to the authenticity and integrity of data bases and the increased potential for exploitation by criminals, activists and terrorists of poorly protected computer systems cannot be ignored and require that immediate practical steps be taken.

The Indian Computer Emergency Response Team (CERT-In)[82]

The Government of India has initiated a comprehensive program to increase awareness of cyber security concerns in connection with the launch of a nationwide CERT, CERT-In. CERT-In has become a central mechanism for increasing awareness of cyber security concerns in India. It has assembled a comprehensive set of background briefing documents and organized several symposium, including a joint meetings between Indian and U.S. experts involving e-security. It has published white papers dealing with spam and phishing issues. It has organized a symposium focused around the role of Microsoft as a software supplier concerned with security issues. In many respects, CERT-In is a template that might be used as a benchmark for other countries seeking to accord higher policy priority to e-security issues and risk management in the business sector.

According to its charter the purpose of CERT-In is to become the nation's 'most trusted referral agency' for responding to computer security incidents as and when they occur as well as to assist members of the Indian Community in implementing proactive measures to reduce the risks of computer security incidents. The CERT-In operates under the auspices of, and with authority delegated by, the Indian Department of Information Technology, Ministry of Communications & Information Technology. CERT-In distinguishes between pro-active and reactive roles and three complementary functions.

Roles

Reactive

— Provide a single point of contact for reporting local problems.

— Assist the organizational constituency and general computing community in preventing and handling computer security incidents.

— Share information and lessons learned with CERT/CC, other CERTs, response teams, organizations and sites.

— Incident Response.

— Provide a 24 x 7 security service.

— Offer recovery procedures.

— Artifact analysis

— Incident tracing

Proactive

— Issue security guidelines, advisories and timely advise

— Vulnerability analysis and response

— Risk Analysis

— Security Product evaluation

— Collaboration with vendors

[82] Information selected from http://www.cert-in.org.in/

- National Repository of, and a referral agency for, cyber-intrusions.
- Profiling attackers
- Conduct training, research and development
- Interact with vendors and others at large to investigate and provide solutions for incidents

Functions

Reporting

- Central point for reporting incidents
- Database of incidents

Analysis

- Analysis of trends and patterns of intruder activity
- Develop preventive strategies for the whole constituency
- In-depth look at an incident report or an incident activity to determine the scope, priority and threat of the incident

Response

- Incident response is a process devoted to restoring affected systems to operation
- Send out recommendations for recovery from, and containment of damage caused by the incidents
- Help the System Administrators take follow up action to prevent recurrence of similar incidents

These outreach efforts means encouraging fundamental shifts in public attitudes about cyber security threats. This can only be accomplished by a multi-pronged intensive corporate relations media campaign actively supported by, e.g., Internet service providers and other stakeholders. Consumers and large scale businesses alike need to be convinced that increased cyber security is not just a remote, regulatory concern. It must be widely accepted as an essential and integral part of information-related and ICT-dependent services.

Before such a multi-prong can be launched, senior business executives need to be convinced as well about the efficacy of a well-focused cross-sector effort to establish new corporate risk management disciplines.

CEOs, Board Chairmen, and the Government ‘CIO’-function have to be brought on board and broadly and publicly acknowledge the long-term importance of improved security. This support should derive from broad strategic commitments rather than micromanagement. It may be based on a broad recognition of the importance of improving ICT corporate governance mechanisms, as an integral part of corporate governance reforms. It may also be based on a commitment to apply rigorously, with active senior level leadership, international standards for information security management including ISO/IEC 17799 as an integral part of the company's overall quality control program. In a more fundamental way, "cyber security" must become accepted as an integral part of whatever products or services the company produces.[83] Finally, corporate support may have to be encouraged and buttressed through a diverse set of sources including the best available intelligence appraisals consolidating both public, semi-public, and private sector generated information. [84]

Given the difficulties of regularly assembling advisory bodies on a face-to-face basis, more attention may need to be given to secure, interactive (web-based) conferencing. High-level industry-oriented advisory groups operating in large nations, regions, or regional institutions (e.g., the European Union) may need as well to take on the case of "recruiting" and building coalitions among senior executives from other CII-enterprises and critical service/sector associations or confederations on a global basis.

The case for improved information security should not be based on security concerns alone. It should be made as a matter of business policy. This may require a different type of institutional advocacy. The senior leadership of the public sector cyber security coordinating entity may need to have in some countries unimpeachable credentials in the business community. In other countries with differing traditions and approaches to public leadership, a coordinator would simply need to champion e-security

[83] ISO/IEC 17799 need to be enhanced to include ICT-based process-control as well.

[84] In the United States, this task needs the impetus of high-level industry bodies like the NIAC and NSTAC which rely on CEO-level membership and the Presidential appointment process. NSTAC-like structure may need to become more multi-sector in orientation and involve not just infrastructure providers but also sectors dependent on such infrastructure. The NIAC committee structure seems to be a step in this direction. This model might be considered in other countries.

concerns and have the necessary credibility with the public, semi-public, and the private sector. The case for improved security—and better risk management in the private sector –may need to be made through industry confederations (such as the British Confederation of Industry, the Indian Confederation of Industry, or the Union for the Coordination of Transmission of Electricity) and by ministries with a trade and commerce portfolio. In India and Russia, leading roles in raising the profile of e-security concerns are being played by industry associations of ICT and software providers, such as NASSCOM in India and RANS in Russia. Independent telecom regulators and e-economy countries can help to make this happen but may not be the lead advocates in the business sector in this effort.

Globalization as Driver of E-Security Policies

Countries that do not yet have very advanced information and communication infrastructures may not be motivated to implement costly e-security policies. However, if their economies are dependent on international trade and foreign investment, this may compel them to revise these policies. Efforts to increase network security may indeed be necessary in order to accommodate foreign trade partners and investors who themselves have become reliant on information and communication infrastructures to conduct day-to-day business.

India, a country that has substantially invested in the development of its own IT capacity, also provides a good example of this international orientation. As reported by NASSCOM[85], the Indian 'National Association of Software and Service Companies' most of the Business Process Outsourcing (BPO) companies providing services to UK customers ensure compliance with the UK Date Protection Act of 1998, companies dealing with US customers ensure compliance depending on the regulation applicable to the industry served. To ensure compliance with regulations, Indian vendors follow security practices as specified by customers such as security awareness, protection of information, non-disclosure agreements, screening of employees, etc. NASCOMM also mentions that many companies have undergone an SAS 70 audit. The Statement on Auditing Standards (SAS) No. 70,, is an internationally recognized auditing standard developed by the American Institute of Certified Public Accountants (AICPA) for Service Organizations.[86]

A central coordinating role requires high levels of skills in building bridges and communication with intelligence and other agencies with sensitive, national security-related portfolios. Because in many countries policy concerns with cyber security or terrorism will significantly influenced by officials with a national security and

[85] http://www.nasscom.org/

[86] http://www.sas70.com/

intelligence background, the policy coordinator will have to have very significant credibility in this area as well as the ability to mobilize mechanisms for international collaboration. This task will also be in competition with other pressing priorities; therefore, policy coordinators will need to find ways to encourage cooperation at all levels **(**strategic, tactical and operational) — and across critical information infrastructure sectors, especially among inter-dependent sectors.

The coordinator must be able to reach out to other ministries or departments with sector-specific oversight of different critical infrastructure services and sectors. Finance ministers, financial services authorities, and banking supervisors will take a specialized interest in the financial sector. Energy ministers and independent energy regulators will jealously guard their prerogatives with respect to electricity, oil, and gas infrastructures; and health authorities are on top of information security practices in hospital and the health care system as a whole. Likewise, independent telecom regulators or ICT-ministers will view their sectors as their own special field of expertise.

The key task of a policy coordinator will be to break down natural tendencies to "compartmentalize" or "stovepipe" cyber security initiatives in a series of separate sectors. There are, and will be, many common challenges and risk factors. Incidents in one sector will have potential relevance in other sectors. The question is how best to bring into concert these separate domains of activity.

CERTs at the national level like CERT-In may be one point of interface. It cannot be assumed, however, that inter-sector cooperation will develop easily or without some external prodding. The case for taking action, as noted above, may rest on a rather technologically sophisticated assessment of potential risk factors relating to the global information infrastructure. The case will require "expert" support along with broad political backing, especially with officials with a national security portfolio. Overseeing the various inter-related roles in an overall security framework is potentially a huge part of the new portfolio of e-economy ministries..

The process of hooking together different pieces of the network may ultimately not be the responsibility of a single coordinator. It is likely to require “collective commitment”. It will require the various counterpart entities to do their parts. The specific roles of these counterparts are briefly discussed in the following sections.

3. Independent Telecom Regulators and IT/ICT Ministers

Telecommunication regulators or ministers with ICT-portfolios may, in a number of countries, be in a very advantageous position to deal with current and emerging cyber security challenges.

In many countries, either the independent telecom regulators and/or ministries responsible for telecommunications policy may have long exercised responsibilities in the area of crisis-related communications. They may have had roles, at times in cooperation with other agencies concerned with emergency preparedness or national defense, in developing and implementing plans for responding to natural disasters or other civil emergencies where demands on basic telecom infrastructure may exceed available resources and capacity must be allocated on a system of priorities. But the dimensions of threats and challenges have grown and are often novel requiring a more inclusive approach than might have been followed in the past.

Nevertheless, independent Telecom/ICT regulators and/or ministries responsible for telecommunications policy are in a position to coordinate industry consensus-building round “good practices” to protect core infrastructure as well as address emerging issues involving mobile and wireless networks.[87]

[87] The role of the U.S. FCC working with industry counterparts through the Network Reliability Interoperability Council is one good example of such a role. In the Netherlands, the Minister of Economic Affairs driven public-private Nationaal Continuïteitsplan Telecommunicatie/ National Telecommunications Contingency Plan (NACOTEL) is another example.

Security Policy and Critical Infrastructure Protection: Approach of Swiss Telecom Regulator, Ofcom

The topic of critical infrastructure protection relating to the telecommunications infrastructure has presented the Swiss regulator, OFCOM, with hard choices. On the one hand, OFCOM has a strong interest and responsibility to ensure the reliability of telecommunications networks and the availability of telecommunications services. On the other hand, the telecommunications networks belong to private enterprise and OFCOM has actually no direct competence to interfere with the running of these networks, e.g. by publishing binding security regulations. The need to find a balanced solution has influenced OFCOM's activities in the area of critical infrastructure protection (CIP). OFCOM has engaged in extensive cooperation with network operators, service providers and other bodies, both public and private, which are active in CIP. Some examples of its activities are set forth below. In addition, OFCOM has proposed that its legislative charter be amended to authorize it to issue technical and organizational regulations relating to security and availability of communications infrastructure. These changes are expected to enter into force during the second half of 2006.

Risk Analysis:

Together with a broad cross-section of the industry and the public sector, OFCOM commissioned and took an active part in a comprehensive risk analysis of the telecommunications sector, the results of which were published in 2004. Following on from this risk analysis, a working group identified a range of measures aimed at reducing the risks and classified risks according to the affected party, their importance and urgency.

Business Continuity Planning:

Having identified a number of risk reduction measures as described above, it was determined to be necessary to ensure their implementation as far as possible. This will require action on the part of the government, the entire industry, as well as individual firms. The industry has jointly initiated an implementation project that is being undertaken under the rubric of 'Business Continuity Planning'. OFCOM takes part in these efforts.

Best Practice Guidelines:

As mentioned above, OFCOM has not acted through binding regulations covering the operation by private enterprise of the telecommunication networks until now. However, Swiss telecommunications legislation does impose some general requirements concerning reliability, availability and quality of services on network operators and service providers. OFCOM has concluded that it is necessary to expand on these general legislative requirements and explain how they should be put in practice. It intends to do this in a next step by means of guidelines for best practices covering the design and operation of networks. OFCOM is currently developing such guidelines as a joint undertaking with the major network operators. The resulting guidelines will – at least initially - not be compulsory requirements but rather a clear practical expression of what is expected from network operators under the law.

Awareness raising for Information security: InfoSurance:

InfoSurance foundation is a public private partnership devoted to information assurance which has been operating for several years. The past year has been a turbulent one for the foundation because its financial support from the industry was withdrawn. OFCOM has been engaged very actively in formulating a rescue plan. By reducing the size of the permanent office and hence overhead costs, binding sponsor support more closely to specific projects and changing the legal form of the organization, it has been possible to ensure the survival of InfoSurance and the continuation of its important work in awareness raising of information assurance problems and solutions with a special focus on Small and Medium Enterprises (SME).

Digital Signature:
The digital signature is a special activity in the security area which falls within OFCOM's responsibility. OFCOM has been responsible for preparing the legislation relating to it. This ranges from changing the law to allow equivalent status of digital and written signatures down to the technical and administrative regulations covering certification services. OFCOM believes that the necessary provisions are now in place to allow increased reliance on digital signatures.

Independent ICT-regulators will build on their existing areas of experience and expertise and, in coping with issues of convergence, will be dealing with the structurally complex Internet sector. The number and diversity of operators and service providers involved in the Internet may be so great that consensus and trust-building may take too long and regulators may need to consider the option of enacting new regulatory requirements. Nevertheless, some independent telecommunication regulators have exercised their mandates to counter activities like electronic fraud, auto-dialers, spyware, and spam. [88].

Regulators will increasingly be required to anticipate the impact of Next Generation Networks on other sectors dependent on telecommunication and Internet services. It is very important to have a first tier of defense against cyber-related risk factors and one that can continue to evolve as communications technologies evolve.

Independent Telecom/ICT regulators must constantly weigh, and use with restraint, their ability to impose regulatory obligations or lead industry debates about standards. They can also encourage private consensus building and leave decisions about implementation to industry players.

Telecom/ICT regulators will continue to rely on the standard setting and other coordinating roles of the International Telecommunications Union (ITU) and other regional bodies such as Commission Interamericana de Telecomunicaciones (CITEL),

[88] For example, see the activities of the Dutch independent telecommunication and post regulator OPTA, Annual report 2004, http://www.opta.nl/download/Jaarverslag_2004_ENG.pdf

APECC, and the European Commission. As noted elsewhere, the ITU has been devoting significant resources through Study Group 17 to issues of ICT cyber security. In addition, both the Organization for Economic Cooperation and Development (OECD) and the ITU have been involved in assessing how the risks of increased levels of spam can be effectively addressed by regulators and other public officials working together. These efforts have resulted in increased contacts and collaboration between regulators and officials responsible for CERTs at the national level. For example, spam has been recognized as a priority concern by CERT-In in India, ICT ministry officials in Russia[89]. and the Dutch telecommunication regulator OPTA in close cooperation with the French privacy commissioner CNIL.[90]

[89] See the Memorandum on Counteracting the Distribution of Malicious Programs (Viruses) and Unauthorized Advertising Messages (SPAM), prepared by the public and governmental Association of Documentary Telecommunications (ADT) on behalf of the commission of the Minister of the Russian Federation for Communications and Information, Moscow, 2003.

[90] E.g., see “Cooperation procedure concerning the transmission of complaint information and intelligence about spam” http://www.opta.nl/asp/en/newsandpublications/backgroundinformation/document.asp?id=1499

International Coordination Efforts in the Asian Pacific[91]

The Asia-Pacific Economic Cooperation, or APEC has been actively promoting international coordination efforts in its region since 2001. APEC is an inter governmental grouping comprising 21 “Member Economies”. Unlike the WTO or other multilateral trade bodies, APEC has no treaty obligations required of its participants. Decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis.

On October 21, 2001 the APEC leaders issued their 'Statement on Counter-Terrorism' that condemned terrorist attacks and agreed to strengthen cooperation in combating terrorism. As part of this statement, the APEC leaders called for strengthening APEC activities in the area of critical infrastructure protection, including telecommunications. On May 30, 2002, the Telecommunications and Information Ministers of the APEC economies issued the 'Shanghai Declaration that included a Statement on the Security of Information and Communications Infrastructures' and a 'Program of Action'. The Statement endorsed action by member economies to combat criminal misuse of information and instructed its The Telecommunications and Information Working Group (TEL) to give special priority to and facilitate APEC work on the protection of information and communications infrastructures.

TEL members have combined their efforts to combat e-security threats under the APEC Cybersecurity Strategy, which includes a package of measures to protect business and consumers from cybercrime, and to strengthen consumer trust in the use of e-commerce. One of these initiatives concerns the development of guidelines to facilitate cross-jurisdictional e-commerce. TEL plays a stimulating role by encouraging and facilitating the sharing of information, the development of procedures and mutual assistance laws, and other measures. The TEL Cybercrime Legislation initiative and Enforcement Capacity Building Project supports institutions in implementing new e-security laws, consistent with the UN General Assembly Resolution 55/63 (2000) and the Convention on Cybercrime (2001). The TEL also plays an active role in stimulating the creation of Computer Emergency Response Teams (CERTs).

[91] http://www.apec.org/

APCERT: Asian Coalition of CSIRT Teams and Brief Profiles of Cyber Security Activities in Vietnam, Korea, and China

APCERT is a coalition of fifteen Computer Security Incident Response Teams (CSIRTs) from twelve economies[92] across the Asia Pacific region. APCERT members get together at annual conferences to report their annual activities, as well as to share and discuss recent incident security issues and future strategies.

APCERT has:

- developed into a dynamic network of responsive CERT/CSIRT contacts which is now one of the best; and the first of its type in the world
- gained the active support and confidence of the many governments in the region and the attention and interest of government and non government regional groups beyond the Asia Pacific region
- been invited to participate and contribute to intra-government forums such as APEC
- become a model for the development of other regional groups in the world and a benchmark for such groups to measure against.
- commenced active sharing of information about computer threats, vulnerabilities and incidents and demonstrated a capability to provide practical and effective incident response across national borders

APCERT Annual Report (2004)[93] includes information relating to APCERT members' annual activities, incident response statistics, analysis and trends, as well as their future plans. Set forth below is a short description of the activities of Vietnam and Korea and China in 2003.

[92] These countries include: Australia, Vietnam, China, Hong Kong, Indonesia, Japan, South Korea, Malaysia, Philippine, Singapore, Thailand, Chinese Taipei

[93] http://www.apcert.org/APCERT2003AnnualReport.pdf

Bach Khoa Internetwork Security Center (BKIS) - Vietnam

According to statistical data available from BKIS concerning Vietnam, more than 90 percent of the PCs in Vietnam were infected by viruses in 2003. In 2003,62 new viruses appeared in Vietnam in comparison with 30 new viruses in 2002. Some typical cases are: W32.Swen, W32.Welchia, W32.Sobig.F, W32.MsBlaster, W32.Opaserv, W32.Bugbear, etc. As soon as these viruses appeared BKIS updated its Antivirus software and sent warnings to all its members and to public media (radio, television, and newspapers).

Activities of hackers were very diverse in 2003. BSIK replied to thousands of email and telephone calls from victims of viruses and hackers. Free antivirus software was downloaded approximately 1 million times from the website[94].

The Ministry of Public Security has been developing plans to establish a Cyber Crime Unit to prevent and to handle cyber crime in Vietnam. In October 2003, an initial conference was organized to identify approaches to prevent cyber crime. By the end of the year , interest in network security began to gain increased interest by government, business and economic organizations in Vietnam. Public media are dealing with this issue more actively; and BSIK continued efforts to raise the awareness and knowledge of the people in Vietnam in the field of cyber security issues. In 2003, BSIK participated in the Cyber Crime Specialized Course at the International Law Academy (ILEA) in Bangkok, Thailand. In this course BSIK was introduced to some techniques currently utilized by hackers and criminals. In addition, BSIK has reviewing security issues in other Asian countries and visited public officials and private sector representatives in the United States to review network security practices there.

Vietnam has been actively develop plans to implement a VietCERT organization.

[94] http://www.bkav.com.vn/

Computer Emergency Response Team Coordination Center – Korea (CERTCC-KR)

CERTCC-KR is a department of KISA (Korea Information Security Agency) that consists of a group of experts to deal with current and emerging information security issues in Korea and the region.. CERTCC-KR promotes information security through mainly technology development and information security procedures.

The activities in 2003 included incident reports and Domestic Computer Virus Occurrence statistics. In 2003 the total number of incidents reports was 26,179 provided by email. The proportion of the reports related to home users was 73% and were mainly related to slammer, open/proxy spam relay (especially proxy spam relay of personnel computers), worms using MS vulnerabilities. There were 85, 023 reports of domestic computer virus occurrence.(This number came from major anti-virus companies in Korea and CERTCC-KR .). 108 types of new virus were found in 2003 and the proportions of Internet worm, Trojan, and Virus were respectively 63%, 28%, and 6%. CERTCC-KR issued 48worm and virus alerts and published 73 advisories, 6 technical documents, and 4 incidents notes.

A Korea Internet Security Center was established in 2003 because CERTCC-KR concluded that the previous incident response system was too passive to reduce the damage from attacks. To prevent incidents effectively, CERTCC-KR needs to detect, analyze, and announce the related information of incidents actively. Therefore a traffic monitoring system and real-time information sharing system have been developed. CERTCC-KR has been developing early detection, rapid prevention, and assurance of cooperation of the incidents response system.

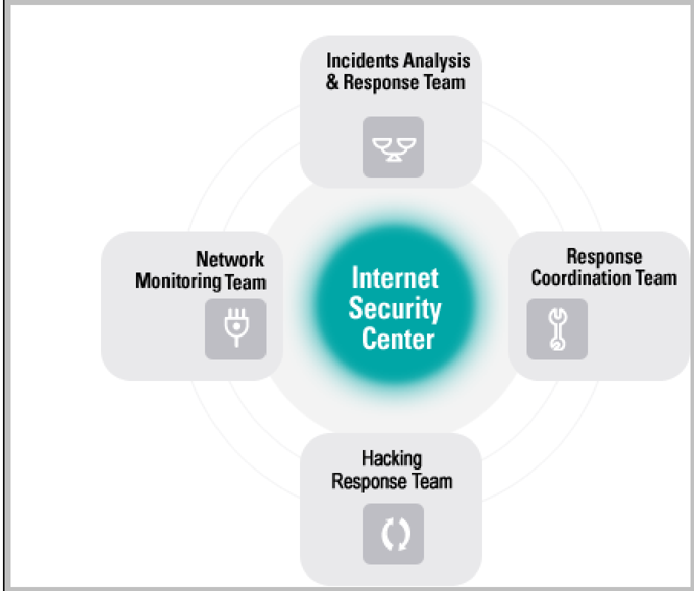


Figure 1. Organization of the Korea Internet Security Center (http://www.certcc.or.kr)

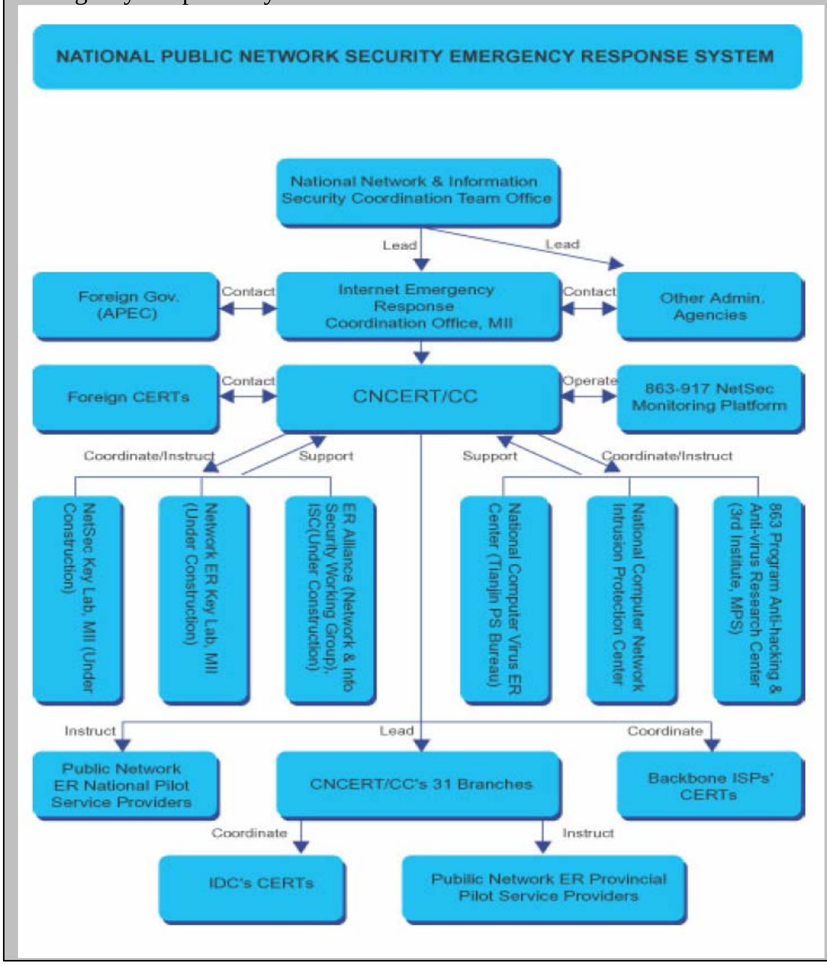
A second new project involved creating a web service through which users can check the vulnerabilities of the web. Since October 2003, every user can access and check on the CERTCC-KR website if his websites are vulnerable. In 2003 CERTCC-KR provided vulnerable checking service to 800 sites.

In 2004 the name of CERTCC-KR was changed to KrCERT/CC. In order to share information in real-time, KrCERT/CC monitors the Internet on a 24/7 basis and increased the accuracy of the system to reduce false positives. It intends to share information with other international CSIRTs as well as the CONCERT (Consortium of CERTs in Korea: 210 members).

Computer Emergency Response Team – China (CNCERT/CC)[95]

CNCERT/CC is a functional organization under Internet Emergency Response Coordination Office of Ministry of Information Industry of China, which is responsible for the coordination of activities among all Computer Emergency Response Teams within China concerning incidents in national public networks. It provides computer network security services and technology support in the handling of security incidents for national public networks, important national application systems and key organizations, involving detection, prediction, response and prevention. It collects, verifies, accumulates and publishes authoritative information on the Internet security issues. It is also responsible for the exchange of information, coordination of action with other international organizations involved with cyber security issues. [96]

CNCERT/CC works as the coordination center of the "National Public Network Security Emergency Response System" of China shown as follows:


NATIONAL PUBLIC NETWORK SECURITY EMERGENCY RESPONSE SYSTEM
National Network & Information Security Coordination Team Office
Lead
Lead
Foreign Gov. (APEC)
Contact
Internet Emergency Response Coordination Office, MII
Contact
Other Admin. Agencies
Foreign CERTs
Contact
CNCERT/CC
Operate
863-917 NetSec Monitoring Platform
Coordinate/Instruct
Support
Support
Coordinate/Instruct
NetSec Key Lab, MII (Under Construction)
Network ER Key Lab, MII (Under Construction)
ER Alliance (Network & Info Security Working Group), ISC(Under Construction)
National Computer Virus ER Center (Tianjin PS Bureau)
National Computer Network Intrusion Protection Center
863 Program Anti-hacking & Anti-virus Research Center (3rd Institute, MPS)
Instruct
Lead
Coordinate
Public Network ER National Pilot Service Providers
CNCERT/CC's 31 Branches
Backbone ISPs' CERTs
Coordinate
Instruct
IDC's CERTs
Public Network ER Provincial Pilot Service Providers

[95] http://www.cert.org.cn/

[96] http://www.cert.org.cn/english_web/document/2004CNCERTCCAnnualReport.pdf

CNCERT/CC’s activities include information collection, event monitoring, incident handling, data analyzing, resource building, security research, security training, technical consulting and. international exchanges and cooperation.

Incident Reports

In 2003, CCERT has received 28,424 incidents reports, more than twice of those of 2002. A taxonomy of statistics of incidents reports is shown in figure 1. More than 62% of these incidents were related to worms, which gave rise to most serious Internet incidents.

Table 1. Taxonomy statistics

1	Virus/Worm	62.87
2	Spam	18.49
3	Scan/Probe	17.36
4	DoS	0.15
5	Intrusion	0.12
6	Unknown	0.46

More than 70% of these incident reports came from Japan and USA. The reports from China domestic account for 8.1%. The source of the reports is classified by the domain name or IP using the APNIC WHOIS database.

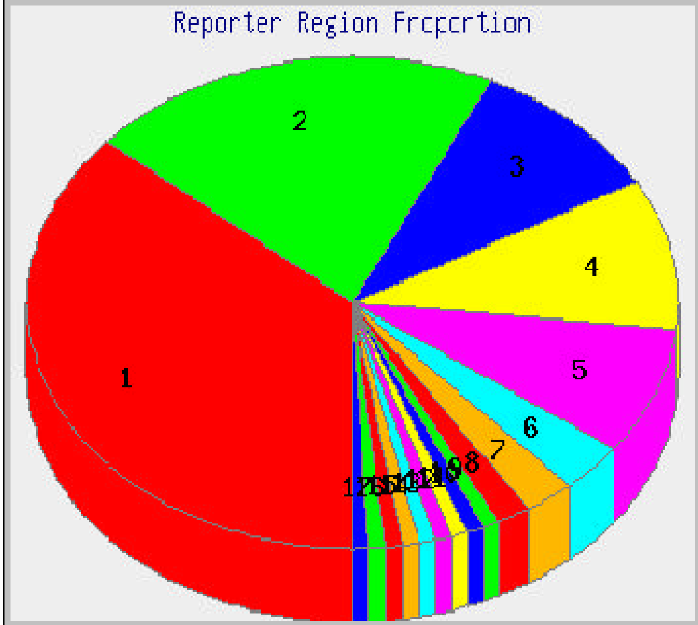


Figure 2 Source of the report

1	Japan	52.0%
2	USA	19.8%
3	Unknown	12.5%
4	Israel	9.2%
5	China	8.1%
6	Singapore	0.9%
7	Canada	0.7%
8	France	0.6%
9	Brazil	0.6%
10	South Korea	0.3%

In response to the most serious incidents, CCERT has published 20 advisories to the users of CERNET in 2003.

The top 10 of the most serious incidents in 2003 are listed as follows:

2003/01/25 Slammer.Worm
2003/03/08 DvlDr32/Deloder/W32.HLLW.Deloder
2003/03/19 CodeRed@F
2003/05/04 A large number of computers were installed with backdoors
2003/06/10 DDOS Attack against some BBS Servers
2003/06/30 Randex.C.worm
2003/08/12 Blaster.Worm
2003/08/19 Nachi/Welchina
2003/08/16 SoBig@F
2003/09/10 Worm_Swen.

An Original Initiative to Promote E-Security Awareness and Competence Building[97]

An electronic news message of CAIS, Brazil's Security Incident Response Team reports that two of its technicians were invited to participate as jurors in the 2005 Second Forensic Analysis Competition organized by the Unam, the National Autonomous University of Mexico and Rediris, a Spanish academic network. The aim of this competition is to foster the development of the forensic field in computing in Latin America and Spain. Still according to this news message, more than thousand individuals or groups were competing for one of the three prizes offered: a license of the software Encase Forensic Edition (1st place), a registration, with all the expenses paid, in the congress Seguridad en Computo 2005 (2nd place) and a registration in a Sans Institute course (3rd place).

[97] http://www.rnp.br/en/news/2005/. More information about the Second Forensic Analysis Competition can be found at the address http://www.seguridad.unam.mx/eventos/reto/

Southern African Economies to Harmonize e-Security Policy and Legislation

There is a delicate balance to be struck between a countries economic reliance on ICTs, the availability technical and financial resources and the necessity to invest in e-Security. An important driver for e-Security policy might be the need to accommodate international trade partners who trade electronically. But even less advanced regions in terms of ICT usage are increasingly concerned with e-security. Their motives are explained in the following article from the Daily News.[98]

GABORONE - The Director of Information Technology (IT) has described the move by Southern African Development Community (SADC) countries to harmonize Internet laws as an indirect call for Botswana to develop its own cyberspace legislation to deal with the increasing use of technology.

[...]

She explained that the amendment entails identifying laws that need to be adopted or changed bearing in mind that wherever possible such laws should be at par with the SADC provisions.

Ramaribana stated that Internet development in the country as a whole, especially digital recognition of electronic copyright on electronic media, depend on the success of Maitlamo, which builds upon Vision 2016 and provides many key strategies essential for achieving Botswanas development targets.

She described this initiative of harmonizing cyberspace laws in SADC as a sensible one, pointing out that it makes sense for SADC countries to have the same definition of what constitute cyber legislation.

The move by SADC countries to harmonize cyber law will ensure cross-border enforcement of cyber crimes such as hacking, computer fraud and online scams, allowing for the extradition of Internet criminals.

Representatives at a recent SADC gathering realized that if the region employed common standards for the collection and presentation of electronic evidence and freely shared such evidence, more criminals would be arrested in the region.

It was highlighted that so far South Africa and Mauritius have already enacted various new laws to deal with the ever-increasing use of the Internet for communication, entertainment and trade whilst most of the SADC member states are in the process of developing their cyber policies.

Organized by the Commonwealth Network of Information Technology for Development and the Centre of Specialization in Public Administration and Management, the recent conference held in South Africa aimed at informing permanent secretaries and public service directors involved in overseeing IT in government.

In countries without well-established regulatory bodies or even well-elaborated cyber security policies, regulators will have to define their roles carefully and identify ways that they can lead, and advise on cyber policy debates without necessarily being the lead agency in the field.

[98] Daily News, 20 April 2005. On-line http://www.gov.bw/cgi-bin/news.cgi?d=20050420&i=Botswana_to_develop_cyber_law

There are, in effect, as a practical matter, some not so bright lines delineating jurisdictional boundaries and areas of responsibilities among agencies dealing with cyber security issues. These "boundary lines" have been the basis for according regulators a clear role and mandate when it comes to spam and less clear roles when issues involving potential threats to critical information infrastructures (CIIs) are at stake. Spam can, of course, generate potential BOT-related threats of denial-of-service attacks against critical information infrastructures. As the spam-issue takes on more national security-related overtones, the jurisdictional claims of telecom regulators –and even regional bodies with policy mandates to support them such as the European Commission—may become more attenuated. European Commission officials point, in fact, to their current lack of institutional mandate to deal with national security-related issues. Some of these jurisdictional boundaries need to be given close attention in devising future policy frameworks.

Independent regulatory bodies would be well-advised to look closely at cyber security-related roles and responsibilities of other regulators and to decide which options and approaches are best suited to their own national context. They will need to appraise realistically what they can and cannot do and what needs to be left to others to manage and lead. Most importantly, they should assess carefully whether and how they can take a leading or influential role in a policy context which requires the empowerment of a wide range of different public, semi-public, and private sector participants. In Part V we have set forth an overview of approaches and initiatives that might be taken by independent regulators.

4. Critical Information Infrastructure Agencies

Ministries or government departments with sector-specific responsibilities can help highlight the importance of cyber security concerns in their respective sectors.

Korea Promotes an E-Security Culture

In 2002 the Korean government published an ambitious vision documents, In this document entitled e-Korea Vision 2006[99] the Korean government announced a wide range of policy measures and institutional initiatives, such as the creation of a Korean CERT.

Noteworthy is the intention to promote e-security in education and to stimulate the creation of a "culture of security". The plan included the development and distribution of educational programs and public relations films for establishing ethical standards on the internet. Education in 'cyber culture' the document continuous, should involve students, teachers and parents.

The government also announced that it will facilitate easier access to relevant information especially for youths through the construction of a special portal and the distribution of a 'white list' of websites. The government announced the distribution of 'selective access software' for internet users and its intention to support activities of civic organizations and information providers, which monitor and review indecent internet content. In addition, the government announced measures against the infringement of human rights on the internet, such as defamation and sexual violence.

They can take a lead in industry discussions making the case from attaching higher priority to cyber risks. They can also operate in a way that contributes to compartmentalization and lack of synergy in response to potentially common sets of risk factors. Such compartmentalization may contribute to CERT or ISAC mechanisms that are narrowly focused on the specific sector within the responsibility of an overseeing ministry. As suggested in Part III above, these information sharing and incident response mechanisms may function more efficiently in a flexible environment permitting a wide range of intra and inter-sector relationships. In many countries, there may also be real concerns in the private sector that potentially heavy-handed ministerial or government involvement might result in requirements or prescriptions with respect to risk management that reflect government priorities but do not make sense from a business standpoint.

How responsibilities are shared between coordinating bodies at the cabinet or cabinet department level and sector-specific ministries or departments will vary greatly from country to country. Approaches to policy coordination will vary among countries

[99] Ministry of Information and Communication (2002). e-Korea Vision 2006: The Third Master Plan for Informatization Promotion (2002~2006), online http://www.ipc.go.kr/ipceng/public/public_view.jsp?num=2007&fn=&req=&pgno=4

with differing administrative cultures and may vary over time as cyber security policies are accepted as a central and high-level policy priority and become better embedded in a broad range of critical information infrastructure sectors.

The right balance between central coordination and policies tailored to differing sector requirements is critical to achieve. One way to avoid internal or bureaucratic differences may be to shift more responsibility to decision-makers at the corporate level. In the early stages of implementing a national cyber policy in India, for example, the Indian Ministry of IT and CERT-In appear to be attaching high priority to improving risk management at the enterprise level.[100]

5. Intelligence and National Security Agencies:

Intelligence agencies are likely to have an increasingly important role to play in developing an overall national intelligence assessment of cyber security risk factors. Such assessment might be offered in a public context or in more closed circle of senior level executives on the basis of classified information. This information may well have a very significant impact on how cyber risk management is undertaken at the corporate level.

Unless "threat assessments" in the field of cyber security have some credible imprimatur and provenance, they are unlikely to be a basis for significant commitments of corporate resources. Senior executives are unlikely to respond to what are viewed as merely speculative risk factors. It is frequently pointed out that the unknowable cannot really ever be known. But when the potential costs are very substantial from both a corporate and a societal standpoint, there may be a sound basis for acting on the basis of speculative scenarios and risk factors. Corporate executives require a well-supported factual and theoretical basis upon which to allocate risk management-related resources.

[100] See various policy presentations prepared for CERT-In in September, 2004 that are focused an enterprise security architectures and risk management policies.

There are, of course, important policy questions concerning how and when sensitive intelligence-related information is delivered to private sector participants.

In the U.S., the NIAC Working Group on Risk Management[101] is working on ways to establish better lines of communications and improved risk assessment methodologies in the public and private sectors. This working group is likely to provide information relevant to a broad range of public, semi-public, and private sector entities around the world.

The National Infrastructure Security Coordination Centre (NISCC) in the U.K. has been established as a cabinet level coordinating committee including resources from defence, intelligence, law enforcement, trade and central government agencies with a mandate to protect critical national infrastructure from electronic attack. This inter-agency body has been the focal point in the U.K. for information sharing through CERTs, a "lighter" alternative to CERTs known as Warning, Advice, and Reporting Points (WARPs), and Information Exchanges.

The latter information exchanges are carried out through face-to-face meetings on a periodic basis and are intended to provide for an informal exchange of views and information among government officials and senior executives in key sectors. NISCC has established various sector-specific liaison relationships and working groups. However, its approach to establishing contacts and information flow relating to cyber threats appears to be more informal, direct, and less bureaucratic than may be currently the case in the United States.

Intelligence agencies are, in many countries, in a unique position to evaluate on an integrated basis public source information, as well as aggregate information from private sector reports, information from third party specialist firms as well as information

[101] NASA Institute for Advanced Concepts.

from a diverse range of foreign sources. Their stock and trade is evaluation and assessment of myriads of disparate pieces of information. However, the effectiveness of such processes depends on whether data from private sector sources is made available.

In some countries, intelligence, and/or national security agencies hold a virtual monopoly with respect to management of information flows relating to sensitive national security concerns. In such countries, such a dominant role by security-related agencies is likely to co-exist with traditions of state ownership and control of strategic enterprises that make it very unlikely that an open culture of risk management will exist in enterprises comprising the national critical information infrastructure. This centralizing of policy responsibilities in ministries or departments that are not at all accustomed to operate on a transparent or non-secretive basis can result in real disparities with cyber security frameworks in other countries that are based on the view that cyber security concerns require a diverse, open, and decentralized, public-private shared management style.

One of the great challenges for policy-makers in the coming years will be to create a better match among very divergent institutional and organizational approaches to dealing with cyber security issues. Because of the need to establish more convergent policies in the cyber security domain in which traditional national security concerns loom so significant, it may be necessary for intelligence agencies in more open societies to help lead the way and establish new modes of collaboration with countries with less transparent approaches to security-related issues. Such new modes of collaboration would be based on a more diverse and open set of international arrangements for dealing with cyber security issues where ties among peer intelligence agencies were not necessarily of pre-eminent importance or the exclusive channel for dealing with new cyber security risk factors.

In Parts IV and V, we discuss possible ways that more effective interfaces among divergent policies and institutional styles can be effectuated in a gradual and exploratory fashion. An effective global scheme of collaboration in the cyber security arena requires that new relationships be woven and that new “connecting paths” for information, among private and public sector entities be established.

The Thin line between Security and Privacy Protection

At a joint OECD-APEC[102] conference in 2003, Mr Stephan Lau, acting in his former data commissioner of Hong Kong, emphasised that 9/11 changed the world. Four trends have become apparent since. These include the swift erosion of pro-privacy laws, greater data sharing among corporations and police, greater eavesdropping, and increased interest in people-tracking technologies. Mr. Lau cited a recent NGO statement that society has shifted from the right to know to the need to know. A poll showed that 63% of US citizens are concerned with increasingly restricted individual freedoms. He welcomed the OECD Security Guidelines for providing timely and appropriate safeguards but also stressed that it is important to respect democracy and ethics principles, and governments and the business sector should go a long way to resolve the tension between security and social values. Mr. Lau concluded with steps that government and business should take. First, openness and transparency are necessary and should be achieved through dialogue, not confrontation because it is important to have joint participation. Second, it is important to remember that privacy enhancing technology can be used to protect identity, but also to violate identity. Third, the commitment to privacy is important and should be promoted to the community at large. Finally, accountability must be an integral part of any security system.

These issues of dealing with structural mismatches in cyber security frameworks need priority attention in order to meet future challenges and close the identified gaps. Moreover, as discussed before, countries in transition from a more controlled to a more open environment may become breeding grounds for various types of grey or black market activities in the cyber arena.

6. Law Enforcement Agencies

Law enforcement agencies have a key role in deterring cyber incidents. The Council of Europe’s Cyber crime convention and G8 action plans have established national law enforcement contact points on a 24*7 basis for cross-border international assistance in case of fighting cyber crime. They have a key role in investigating suspicious activities through sophisticated forensic techniques. Unfortunately, investigative procedures and techniques has not kept pace with the dynamics and speed

[102] Quoted from OECD-APEC (2003). OECD-APEC Global Forum: Policy Frameworks for the Digital Economy. Summary Report Honolulu, 14-17 January 2003.

of modern technology: thus after-action analysis is feasible only in the most important cases.

Furthermore, senior policy-makers do not put cybercrime, from a strategic standpoint, on a par in law enforcement terms with other forms of crime with equal potential for societal damage. There is vicious circle at work. As cyber crime is not well understood, low priority is attached to dealing with it with the result of less training and education, and so on in a downward spiral. Unfortunately, after obtaining more willingness from the private sector to ask law enforcement help, law enforcement is being overwhelmed with incidents. As long as there is not consistent long-term tracking of cyber crime undertaken in an agreed international format, priorities will never be set right.

The Cyber Task Force in the Japanese National Police Agency has established a network of "honey pots" and remote sensors to monitor computer-generated efforts to penetrate corporate and government networks. This group also will audit on a periodic basis the vulnerability of corporate networks sometimes working in parallel with ministries with sector specific responsibilities.

Given the cross-border nature of cyber criminal activity, it is critical to establish effective networks for exchanges of information and expertise. Through a regional organization of ministers of justice and attorneys general, the OAS has encouraged an exchange of know-how and expertise relating to new legal frameworks necessary to investigate, prosecute, and deter cyber criminal activity. Countries like the UK[103] and the Netherlands[104] have formed National High-Tech Crime Centers which concentrate on analyzing cyber crime patterns. These centers involve public-private cooperation between a large set of government departments and agencies as well as private industry.

[103] http://www.nhtcu.org/nqcontent.cfm?a_id=12261

[104] http://www.nhtcc.nl/index_en.html

Interpol actively involved in e-Security[105]

Interpol has been involved in combating Information Technology Crime for a number of years. The Interpol General Secretariat has harnessed the expertise of its members in the field of Information Technology Crime (ITC) through the vehicle of working parties that consist of the heads or experienced members of national computer crime units. These working parties have been designed to reflect regional expertise and exist in Europe, Asia, the Americas and in Africa. All working parties are in different stages of development. These working parties are not Interpol but represent the most noteworthy contribution to date.

At the occasion of Interpol's 6th International Conference on Cyber Crime in Cairo on 15 April 2005o the delegates recommend:

- That the Convention on Cyber Crime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages.
- That Interpol shall enhance its efforts within the Training and Operative Standards Initiative in order to provide international standards for the search, seizure and investigation of electronic evidence.
- That training and technical assistance should remain a priority area for international efforts against cyber crime, including the development of appropriate training courses and the setting up of an international network of training institutes and trainers involving the optimal utilization of tools and programs such as Interpol's Mobile Classroom and e-learning modules. The training and technical assistance initiatives should be cross-sectional, involving public-private partnerships, including with academia.
- That the vital co-operation and communication between supranational institutions, such as the United Nations and others, as well as national entities fighting cyber crime have to be initiated and developed and speed of response be encouraged.
- That information on cyber crime cases shall be collected in the Interpol database and disseminated in the form of analytical products to assist member countries in adopting appropriate prevention strategies.
- That Interpol Working Parties on IT Crime shall be created in all regions where currently no such groups exist. The expertise available within the existing groups should be utilized to support the creation of such new groups.
- Interpol IPSG shall organize a conference including representatives of the different bodies working in the area of criminal justice in order to achieve a framework for joint co-operation in the field of fighting cyber crime.
- And, therefore, Interpol should take the lead in promoting these recommendations which are vital to effectively tackle information technology crime and protect the citizens of the world in cyber space.

[105] http://www.interpol.int/Public/TechnologyCrime/default.asp

These law enforcement-driven efforts need to be blended into an overall framework on a seamless basis. This will take skill and diplomacy by all participants to avoid bureaucratic infighting and stove-piping

7. Computer Emergency Response Teams (CERTs) and ISACs

As set forth in Part III above, CERTs have become, and are becoming, the critical backbone for preparing for, and responding to, cyber incidents of all types. CERTs are in varying stages of development in industrialized and developing economies around the world. They are more highly developed in some sectors such as the financial services sectors and are being given high priority in public utility sectors that are dependent on SCADA-systems. CERTs are often embedded within the institutional and organization architecture of enterprises of differing size and geographic scope. CERT organizational structures can be based on centralized, decentralized, or hybrid models and can involve significant outsourcing and reliance on commercial firms with CERT-related capabilities.

CERTs can offer a range of services and capabilities. Some may be limited to providing information sharing and analysis and are often referred to as ISACs. Others may offer specialized capabilities to respond to cyber incidents. They collect reports of incidents and vulnerabilities. They act as a point of liaison with software, hardware, and other service providers as well as other CERTs. They generate a trusted body of technical expertise to help evaluate potential incidents and assist their potential constituency. They establish relationships of trust with other public and private CERTs in other organizations, sectors, or countries and deal as a practical matter with potential concerns relating to disclosure to their constituencies or public of potential incidents and network vulnerabilities. They may collaborate on a multi-tiered basis with a range of companies and public and private sector related organizations including ISACs. They are a critical hub for many types of information flows involving a wide range of incidents and different participants. It is critically important for them to have effective collaborative and, above all, trusted arrangements with counterpart CERTs anywhere as well as established procedures for managing incidents with a significant international dimension.

CERT Collaboration among Organization of Islamic Conference Member Countries

At least six of the Organisation of Islamic Conference (OIC) member countries have established collaborations with either the Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT) worldwide to protect their digital assets from hackers. Malaysia's National ICT Security and Emergency Response Centre (NISER) director Lt Col Husin Jazri said the countries were Bangladesh, Brunei, Indonesia, Malaysia, Pakistan and the United Arab Emirates (UAE).

He said OIC member countries could get benefits from the collaborations with CERT/CSIRT through access to the dissemination of cyber alerts on hackers to the widest possible audience.

Organisation of Islamic Conference (OIC) members should set up Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) to collaborate and prevent or reduce cyber terrorism. "Such collaborations will provide a platform among the OIC countries to exchange ideas and expertise about computer threats, vulnerabilities and incidents. It will also demonstrate a capability to provide practical and effective incident responses across national borders," he added.

The NISER director called on delegates at the 30th annual meeting of the Islamic Development Bank (IDB) Board of Governors to pass a resolution to set up the OIC-CERT.

Husin said this while moderating a plenary session on cyberspace safety at the Knowledge and Information and Communications Technology for Development 2005 Conference (KICT4D) 2005, which had standing room-only for participants from Nigeria, Tunisia, Senegal, United Arab Emirates (UAE) and Pakistan as well as Malaysia.

Noting that only seven of the 57 OIC members have CERTs or CSIRTs, he asked OIC members (of which the IDB is the investment arm), to contribute to an OIC-CERT collaboration, setting up an OIC-CERT task force and an interest group forum.(Malaysia has three CERTs: MyCERT for Malaysian Internet users; GCERT for federal, state and local governments, as well as statutory bodies; and Sabah CERT for users in the East Malaysian state.)

Associate Professor Dr Ibrahim Kamel of the College of Information Systems at Zayed University in Dubai, UAE, noted that five West Asian countries (UAE, Kuwait, Saudi Arabia, Egypt and Iran) are among the top 10 countries vulnerable to hacking (Symantec Report 2003).

Ibrahim pointed out that more nations are adding computer network warfare to their strategies, criminals are using cyberspace and critical infrastructures have become prime targets.

As NISER's Husin stressed, "It's not 'Will I get hit?' but it's a matter of 'When will I get hit?'"

OIC-CERT could increase the dissemination of cyber alerts, provide a platform to exchange ideas and expertise, jointly develop measures to deal with large-scale network security incidents and address information security and emergency response across regional boundaries, Husin said.

CERTs are, in effect, the institutional instruments for implementing predominantly at the operational level and sometimes at the national tactical level the overarching policy priorities relating to cyber security policy that may be formulated by the various array of homeland security, intelligence, national security agencies, regulator, and other bodies described above. They are a kind of “gearing system” that generates critical information streams flowing into, and out of, decision-making circles in private corporations or other institutions responsible for protecting critical information infrastructure. .

In assessing different stages of development of cyber security frameworks in emerging markets, a number of factors need to be considered. These factors include but are not limited to (1) the existence of a national CERT, (2) the role of CERTs in key sectors such as financial services or public utility services (focusing on SCADA systems), (3) the dissemination of CERT-related capabilities into key firms in the national economy, (4) the awareness of ICT-related risk management techniques in firms and sectors, (5) the development of CERT-capabilities relating to telecom infrastructure or Internet capabilities, (6) the inter-linkages of such systems with overall national security or homeland security mechanisms, (7) the relationships of CERT mechanisms and intelligence agencies, (8) the patterns of cross-border collaboration and information sharing across the hierarchy of "national nodes" as described herein taking into consideration the experience of different countries.

There are likely to be a number of different "driving factors" that may determine in differing countries which parts of an overall "cyber network" are likely to develop most rapidly. For example, in some countries like India, pressures from trading partner relationships relating to outsourcing in the IT-sector have energized IT-industry associations and IT-Ministry officials to take a leading role in delineating cyber security policy. In other countries, concerns about cyber crime have resulted, as has been the case in Nigeria, in the creation of a special working group dealing with strengthening institutional arrangements for dealing with cyber crime. These initiatives have spill-over effects with respect to other areas of cyber policy.

8. Coordination Among Entities in the Private Sector

Many of the critical interactions among private sector entities are described in detail in Part II hereof.

The discussion below highlights the following points or nodes of coordination: (1) individual enterprises in diverse sectors including the entire "chain of command" relating to risk management within an enterprise, 2) firms in "value chain" or other distribution arrangements with an enterprise, 3) other firms in the same industry sector, 4) suppliers of hardware, software, or services to the enterprise, 5) third party advisors concerning cyber security or risk management including insurance companies, 6) formal or informal industry bodies linking together executives at differing levels of responsibility for the risk management process including CEOs, CIOs, ICT-professionals, etc., or associations of ICT-professionals. All of these nodes are critical “points of intervention” through which initiatives can be undertaken to improve the overall level of cyber security on a systematic basis.

In all these relationships involving the private sector, cyber security issues are dealt from a variety of different perspectives. Some issues deal mainly with a strategic level of concern, i.e., (1) the priorities attached to cyber security and ICT-risk management , (2) high-level corporate perspectives relating to security as an integral part of a firm’s products or services, (3) perspectives about the importance of collaboration with (i) peer firms or (ii) government agencies including intelligence agencies. These concerns relate to vision and leadership. Other areas attracting the attention of policy-makers have a more operational focus such as the organizational or institutional structures for intra-corporate CERTs and ISACs, or the priorities that attach to various multi-tier security models, international standards, or cyber security insurance. It is agglomeration of these concerns—strategic, tactical, and operational—through which the overall framework for dealing with cyber security concerns at the national, regional, and international levels can be significantly improved.

Individual enterprises are essentially the bedrock of effective cyber security policies. However, the approach of such enterprises in dealing with cyber risk factors can differ significantly. It can depend on a range of factors including (i) regulatory oversight and supervision, (ii) corporate governance traditions and policies (iii) competitive conditions, (iv) the degree of social responsibility or political responsiveness that is embedded in the corporate practices of different countries.

Information flows among private sector participants will follow different patterns depending on the nature of the issue involved (i.e., incident responses, threat assessment, vulnerability assessments, initiatives to anticipate and prevent incidents, warning circles, etc.), its potential gravity and consequences (which may be evaluated on an ongoing basis over time) and international dimensions. Many of these inter-actions and information flows will be visible only to a small circle of trusted participants. Depending on the level of incident or concern, they may involve progressively higher level of public and/or private stakeholders in both a national and international context.

Information flows are necessarily dynamic and changing in scope. They can be facilitated or hindered by inter-dependent initiatives of the various participants in the overall "network model" through which cyber security concerns are addressed.

Public officials usually cannot, and should not, direct initiatives taken with an enterprise. Sometimes, they can and do, for example. They can often influence the priorities of a risk management process as well as the range of issues or concerns that might need to be addressed.

Acting in concert with leadership from e-economy ministers and others with special areas of expertise, public agencies can have an impact on market expectations and perceptions about the importance of cyber security including continuity —and fundamentally its integral relationship with core products and services delivered by enterprises.

In an earlier era, product safety concerns relating to crash-worthiness were seen as matters of peripheral concern. Today, no auto manufacturer would envision selling cars without seat belts or other crash protection capabilities. Thus, it is important to distinguish between information flows that are essential to manage or direct various specific cyber-related activities as well as those that change market expectations and the way that all market participants behave with respect to cyber security concerns.

The focus on information flows within the private sector and among any private, semi-public, and public sector participants can help policy-makers "visualize" the systemic and inter-related nature of an effective cyber security framework. It can assist different participants in different parts of an overall network “see” better the entirety of a problem and the ways that actions of an individual firm or entity are likely to impact the decisions and responses of other participants.

Such an overview is likely to be particularly useful from the standpoint of a minister or independent regulator with a broad portfolio dealing with national e-security, e-economy policies, or the e-economy. It makes it easier to identify what an individual minister can do independently and what actions must be encouraged to be taken by others not under his (or her) direct control. It emphasizes as well the importance of communications both of specific directives and instructions as well as broad concepts or ideas that might change the approach of other participants in the overall arrangements for dealing with cyber security. Additionally, a network-oriented policy perspective focuses on the fact that the range of potential actions or initiatives that are likely to be taken in a national context might be reflected in policies and initiatives being taken in other national and international settings. By focusing on “key elements or objectives”, “nodes” and “information flows, it may be easier to “look through” differences in institutional culture and arrangements at what is generally agreed to be important to do. An effective policy framework for cyber security should focus on shared communications not merely of what might be viewed as “best” practices. It should highlight what some experienced policy-makers describe simply as “good practices”.

Identifying these practices and making them widely available is thus a key exercise, and a very critical part of establishing effective cyber security policies. Set forth below in Part IV are some practical steps that might be followed in developing such a body of “good practices”.

V Approaches to Improving Collaborative Networks for Dealing with Cyber Security

Among the advantages of a “network model”, as set forth in Parts II and III, is that it can be used as a benchmark for analyzing and classifying practical experience in different countries dealing with cyber security.

There is already available a rich body of information relating to organizational and institutional arrangements, especially in a number of industrialized countries, that has been collected by the OECD and other organizations . However, this inventory of differing national practices needs to be substantially widened in scope. More information needs to be collected concerning how cyber security issues are actually handled and what might constitute “good practices” of potential relevance to other countries. I We believe that it would be useful for a collaborative group of research institutes or organizations to further “test” the efficacy of this network model and better understand how it might be used in assessing the strengths and weaknesses of the ways that cyber security issues are dealt with in practice.

This study should be the beginning of a process to develop and further refine the network model. This process should be continued through an ever-widening circle of consultations involving other research institutes or national cyber security policy centers. As consultations progress and key principles are tested, the core base of information and analysis collected in the course of preparing this discussion paper and included in the wiki site we have developed can be widened. Such an iterative process will hopefully begin “on the margins” to energize changes in perspective and new institutional initiatives. A well-structured and on-going study process organized around a diverse group of research institutes can, and should, strengthen the international collaboration and new policy initiatives concerning cyber security.

Nationally and Internationally Oriented Collaboration and Research Networks

Models already exist in some areas that could help developing countries structure and focus their burgeoning cyber security research capabilities. The Institute for Information Infrastructure Protection (I3P) in the United States, for instance, brings together the leading U.S. academic research institutions, national labs and non-profit organizations to jointly help address information infrastructure security challenges.

It may be worthwhile to explore such a model in more detail and examine its possible application to research and development (R&D) capabilities in other countries. The basic idea is to unify existing cyber security R&D efforts in a country and focus them toward supporting high-impact national research goals. Such research clusters could be highly effective in maximizing capabilities otherwise spread out across a country (or even regionally or internationally) and applying them in the form of a virtual research network that has common research aims.

A central component to such a model is close cooperation with both industry and government agencies. To be effective in supporting national cyber security priorities, such a virtual research network, or cluster, needs to closely coordinate its efforts with governments, while maintaining a level of academic independence that is the hallmark of research excellence. Close cooperation with government can work in a relatively sophisticated, structured system, but also in developing countries, where there may not be a centralized department of homeland security. In such cases, the government coordinating body could be a telecommunications ministry, an interior ministry, or another body responsible for cyber security at the national level.

As mentioned above, while coordination with government is crucial, a perception of independence is equally important to ensure that researchers retain unhindered access to private industry. This is a delicate balance and needs to be well-managed. Access to industry is pivotal because a good deal of world-class research is carried out in the private sector (by companies). Cooperation with industry will, therefore, help improve the quality of academic research and ensure that findings and technologies are actually applied in the real world, rather than gathering dust on the shelf. Existing efforts to form research clusters or networks have clearly demonstrated that implementing strong technology demonstration and technology transfer programs adds significant value to R&D efforts and brings research to bear directly in areas of acute need.

If implemented correctly, such research clusters should help bring both industry and government to the table to work jointly on articulating high-priority national research needs and sharing information about vulnerabilities, threats and trends in a more trusting environment. In such a scenario, the research network can act as an 'honest broker' between industry and government. Likewise, funding for such a research network can come from government coffers as well as from the private sector. This is particularly attractive because governments often have limited funding available for cyber security and much of the infrastructure that needs to be secured is in private ownership anyway. Whether the government or industry should provide initial start-up funding to establish the research network is a question that is probably best answered in the context of each country where the concept will be applied.

The incentives for government and industry to want to establish such a focused research group are clear. It becomes easier to gain access to the leading researchers and institutions and to help shape the national research agenda in order to develop urgently-needed security tools and technologies. But researchers also benefit from the arrangement.

Through such a research network, researchers can more easily exchange ideas with their peers and self-select into smaller groups to work on specific challenges. The cluster additionally provides researchers with access to a pool of public and/or private research funding. The concept of the research network, cluster or consortium - however one chooses to call it - can be applied at the nation-state level, regionally or even internationally. However, further study is necessary to deal with issues of coordination and control that an international network is faced with.

1. International R&D Coordination Networks

The European Commission has entered into a contract for a so-called coordination project “Critical Information Infrastructure Research Coordination (CI^{2}RCO)” which aims to coordinate R&D on critical information infrastructure protection in the various European countries. The project is to develop an inventory of current and planned R&D activities, and create networks of researchers in specific research areas. Outreach activities with other nations such as the U.S., Canada, and Australia are planned.[106]

It may be useful to explore ways to establish better collaborative ties between research consortia in industrialized countries like i3P, CI2RCO, and ETHZ (Zurich) and research centers in a wider circle of countries including, for example, India, China, Russia, Brazil, and South Africa.

Australian CERT Capacity Building Project

The Government of Australia has established a project for “in-country” CERT training and funding for communications networks as well as fostering the exchange of operational information and technical advisories among several Asian countries. A similar activity is being undertaken by the Australian CERT in Chile, Peru, Mexico, the Russian Federation, Vietnam, Indonesia, Thailand, and the Philippines . These multi-country initiatives are likely to provide a good mechanism through which to collect a more comprehensive data relating to these countries and to examine the role of the CERT in the overall “cyber network” relationships in each of these countries. This project might provide a good basis for a group of international organizations including the World Bank, the European Commission, and the OECD to collaborate together in order to add to the scale and broader international impact of the important initiative taken by the Government of Australia.

2. International Collaboration Networks

A core group of research institutes and national policy organizations with an interest in developing more collaborative international approaches could form a working group and institutional base for future “cyber exercises”.

[106] See CI2RCO description, e.g. in: http://www.computerworld.com/printthis/2005/0,4814,101160,00.html

These “exercises,” which could be conducted under the auspices of the “working group of research institutes” outlined above, would be intended to develop additional background information and understanding of how “collaborative cyber networks” work in different countries and how they might work together. The only way to find out how a network might “react” in some future case is to attempt to identify and “activate” the likely response mechanisms in a hypothetical case and then collect and analyze the results. The key result of such an exercise is likely to be both the collection of additional information and data as well as the development of some “new procedures and practices”.

Set forth below is a proposed approach to developing exercises as an important element of an overall cyber security policy framework.

3. Exercises

Scenario-based exercises are an important tool for developing policy frameworks at the local, regional, national, and international levels relating to the protection of critical information infrastructure. There are a wide range of approaches to structuring exercises; however, we have outlined below three different types of ways that policy-makers can utilize exercises in the process of establishing new policy frameworks. They involve (1) the use of various pre-exercise planning procedures, (2) so-called “table top” exercises, (3) piggy-back exercises ,and (4) various more complex, multi-day exercises. The potential advantages and disadvantages of these different approaches to exercises are discussed in further detail below.

The body of web-related resources assembled as part of the background information behind this discussion paper includes a very comprehensive set of documentation concerning the structuring and use of cyber security exercises that should be of assistance to policy-makers interested in implementing a program of exercises.

Pre-Exercise Planning Session; A pre-exercise planning session is an initial option that policy-makers might wish to pursue and would engage various key public and private sector participants in assessing various options for conducting one or a series of exercises. Such a session might consider various case studies relating to the exercise programs that have been or are likely to be conducted in other countries. Such a planning session would provide a basis for key decision-makers in the private sector as well as in a range of public agencies including ministries responsible for IT and telecom regulatory matters to begin to map out their respective roles in relation to one another. The "network model" discussed above provides some general parameters and guidelines with respect to the differing roles and responsibilities of various public and private sector agencies.

Experienced participants in exercise planning are very much inclined to recommend that the "oversight" and "ownership" of exercise planning cannot be provided by outside experts and advisors. The role of such outsiders must only be to facilitate, and assist in, the putting in place of exercise coordination and leadership arrangements within each national setting. However, it may well be that experienced policy-makers from other countries that have already established an exercise program can provide useful guidance from an outside perspective through first hand or "virtual" consultations.

The practical, first hand experience developed in doing the initial planning for an exercise can give increased impetus to more traditional bureaucratic steps to improve existing cyber security policy and institutional arrangements. It is not unusual to commission internally—or with outside advisory or consulting advice—reports that describe and delineate current and potential frameworks for the protection of critical information infrastructure. However, the very process of organizing a planning session for an exercise is likely to require policy-makers to identify the critical institutional players as well as document any existing initiatives already being taken to deal with network security issues.

An exercise planning effort would certainly complement initiatives to establish or rationalize the operation of CERTs already in operation and help these entities to delineate procedures for dealing with cyber incidents. Moreover, an initiative to organize an exercise program would provide an opening to start a dialogue with key private sector or public providers of critical infrastructure about risk management techniques within such public enterprises and with their key suppliers or customers. Careful documentation of an exercise planning program could help establish the key elements of an overall national cyber security program. One of the key roles of ICT-ministries and telecom regulators might be to work with other agencies concerned with emergency preparedness and national security issues to put in place such a program. The basic steps in establishing an exercise program could be part of a tool kit with which such officials might be provided as a result of any World Bank-led effort to raise awareness about cyber security concerns.

Table-top Exercise Planning: . Table top exercises provide an opportunity for a further delineation of a policy framework for dealing with cyber security concerns on a national as well as on an international basis. They involve the creation of scenarios for various types of cyber incidents or attacks that allow the likely participants in response to such events to identify and assess potential consequences and required responses.

For example, policy-makers may be able to visualize more concretely the range of collaborative ties and lines of communications that may need to be established to deal with a potential cyber attack. Many of the procedures are likely to involve operational relationships among providers of underlying telecom and IT-infrastructure and public and private sector users of such infrastructure. Since attack or incident scenarios are likely to involve private sector firms or state-owned enterprises operating critical infrastructure, there will be a critical need for effective communications and coordination among governmental officials responsible for national or homeland security and key personnel involved in responding to an attack from an operational standpoint. It is also likely to be critically important to determine the source and scope of any potential incident. Is the incident confined to a particular firm or group of firms in a sector or are there potential consequences in interdependent or even independent business sectors? Is there any reason to believe that the potential attack is ‘localized” in nature or part of a more comprehensive attack scenario with international implications?

Though a table top exercise may be confined in scope and have a necessarily "hypothetical" dimension to it, it may help identify the key linkages and lines of communications that are likely to be important to establish in the event of a real incident. The exercise can assist in providing more concrete input to the "network model" described elsewhere in this discussion paper by focusing attention on critical processes and procedures and key flows of information.. In principle a hypothetical scenario can be helpful in encouraging key players in a "networked relationship" to identify their critical counterparts, their respective obligations and expectations, and a likely high priority set of initiatives to be taken in the event of a crisis. Key contact personnel can be identified; contact numbers and procedures can be verified. Procedures for handling coordination and communications in the event of disruption of ordinary lines of communications can be developed. Where there are institutional "blockages" or where no clear-cut counterpart relationships exist particularly in a cross-border context, these potential areas of concern are likely to be more effectively addressed once they are identified in an exercise.

A table-top exercise also allows a range of different participants to "act out" their respective and varying roles in the complex web of relationships required to maintain an overall effective cyber security policy. A table top exercise can focus in on top-level coordination relationships among telecom regulators, ICT-ministers, and homeland or national security entities. Alternatively, it can help delineate a range of lines of communications within and among firms in critical information infrastructure sectors as well as potential cross-sector ties. It can deal with cyber security attack scenarios on a bottom up or top-down basis. Importantly, as well it can deal with sensitive interactions required among senior level private sector representations and public officials in a range of agencies including those with national security and intelligence responsibilities.

It may certainly be easier, in dealing with hypothetical scenarios, to highlight the potential importance of information flows relating to risk management and crisis response than in the context of an actual cyber security attack scenario. It might be possible to lay the ground work for more routine and effective flows of risk-related information between the private sector and public sector agencies with a mandate to monitor and assess the potential for improbable but enormously detrimental risk scenarios affecting the functioning of key industry sectors. See discussion in Part II above relating to the role of intelligence agencies in threat assessment.

Piggy-back exercises; These are scenario-driven exercises where, in connection with another emergency management training exercise, part of the critical information or telecommunication infrastructure is declared to be seriously hampered or disrupted by a physical or ICT-based attack. The training effect comprises elements of other exercises mentioned above: test of emergency communications, alternatives, reachability and effectiveness of information sharing and decision-taking by key officials responsible for cyber security and critical information infrastructure protection. Such exercise also evaluate how emergency management procedures adapt to failures of critical information infrastructures.

Multi-day, complex exercises: These exercises can be carried out over a multi-day period with participants located potentially in a diverse number of locations. The fact that participants are in diverse locations results in the exercise focusing significantly on the effectiveness with which communications tools and other communications capabilities are exploited by participants. Exercises even in a multi-venue, multi-day environment still involve the use of a controlled communications environment. Nevertheless, policy-makers are often well- positioned to evaluate potential bottlenecks or other liabilities relating to crisis management that would be a consequence of cyber-related attacks that might adversely affect backbone communications capabilities.

Multi-day, multi-venue exercises also necessarily require higher levels of political clearances and approvals because some critical personnel may be diverted from day-to-day responsibilities. The preparation time and costs of such exercises can be significantly in excess of that of a table top exercise. It is also significantly more difficult to monitor and annotate the performance of participants in a multi-venue exercise scenario. Typically, feedback is provided both by direct participants as well as by a core of observers who attempt to assess and diagnose any institutional or other issues that may warrant further discussion and analysis.

As suggested above, exercises may be useful at differing stages of development of an overall cyber security policy framework. Their potential utility may not be limited to countries that have already put in place an overall framework and are keen to increase readiness and improve the effectiveness of existing policies. It may also be useful as an integral part of the initial process of establishing a cyber security framework. An approach centered around empowering officials to take various organizational and institutional initiatives –even in hypothetical scenarios--may ultimately prove more effective than a process of drafting white papers and dealing with cyber security frameworks in a more abstract context. Any initiative based on relying on exercises as a policy making tool attaches great importance to the role of outside advisors as facilitators rather than implementers of an exercise program. A number of international research institutes have had important experience in such a facilitative role. It may be useful to link outside facilitators with officials in countries that may have effectively launched an exercise program to form a corps of resources available to countries interested in developing their own exercise program..

As suggested elsewhere, a framework for collaboration among international research institutes could also provide a multi-national platform through which international cyber security exercises could be conducted. There are, of course, many possible ways of conducting international exercises through existing regional or other international organizations. However, given the fact that cyber exercises have many elements in common with various war game scenarios with which national as well as regional security agencies have developed expertise over the years[107], it may be promising to examine ways that these established platforms for contingency planning

[107] An example is the German public-private CII CYTEX exercise as described in http://www.iabg.de/presse/aktuelles/mitteilungen/200111_cyber_terror_exercise_en.php

relating to national security risks could be tailored to deal with the many novel dimensions of cyber security challenges. Such novel challenges may require a different paradigm for international cooperation than has, to date, been the basis for conventional national security contingency planning.

There may be an important role for a consortium of international research institutes, with the support of the World Bank, to play in building bridges across political divides that are a residue of the end of the Cold War or a consequence of current geo-political tensions. These divides may continue to impede effective collaboration among countries that eye each other as potential rivals in a new economy driven by the growing importance of ICT in critical industry sectors. A research consortium might assist in opening up more effective dialogue and discussion—and better meshing of mechanisms for dealing with cyber security challenges-- among the United States, Europe, Russia, and other countries which share concerns about terrorisms but may not have fully convergent views with respect to grappling with the potential linkages between international organized criminal elements and the vestiges of old regime state security mechanisms. It might likewise provide an impetus for better cooperation and better mutual policy delineation among public and private sectors entities in the United States, Europe, and the People's Republic of China. Such cooperation would inevitably embrace closely inter-related relationships on a regional basis including Japan, South and North Korea, and the APEC region as a whole.

The evolution of better collaborative relationships—and more effective cyber security policy—would have a significant spill-over effect affecting countries with significant economic and trading relationships with countries which are at a more advanced stage of introducing ICT into critical information infrastructure.

Security Mock Training Exercise with China, Korea, and Japan

The Korean Government initiated a security violation mock training exercise with the participation of the China, Korea, and Japan in the second half of 2004. This exercise program was organized within the framework of the first Korea-Japan-China Working Level Meeting on Telecom Network Security and Information Security. A task force on information security training and security violation responses has been established between the three countries. This initiative involves an exchange of information on a regular basis on traffic, cases of security violations, and trends relating to

Source: OECD Documentation

VI Key Policy Options and Recommendations

Our recommendations are clustered in three main areas:

- Strengthening the international cyber policy framework

- Some "key recommended perspectives" on cyber security policy for ICT sector officials and their counterparts in other government agencies

- Initiatives to develop enabling resources to develop cyber security policy frameworks in a national and international context.

A Strengthening the International Framework for Dealing with Cyber Security Concerns

We examine below a number of areas relating to restructuring a more effective collaborative international framework for dealing with cyber security concerns:

(1) Key Elements of a Well-Balanced Approach to Cyber Security Tailored to the Complexity and Unique Challenges Facing Policymakers

Cyber security policy must be framed in a complex and turbulent crucible of potential conflicting policy concerns which involve a myriad of different public and private stakeholders both in a national and international context.

To deal with the complexity of the challenges, national cyber policy must:

- have a strong international dimension;

- orchestrate the "interconnected" spectrum of stakeholders—across agency "jurisdictions" and responsibilities and the boundaries of the public and private sectors;

- require each stakeholder to take responsibility and be accountable in its own domain;

- discourage "stovepiping" and compartmentalization of responsibilities;

- recognize that cyber security policy has many "faces" or aspects including

  (i) national security concerns about international conflicts and terrorism and the protection of critical information infrastructure;

  (ii) protection of such critical infrastructure from organized criminal activity that may or may not have rogue state sponsorship or a nexus with terrorist elements;.

  (iii) Ensuring the flow of new investment, the developing of international trade and finance relationships, as well as promoting economic growth and improved delivery of public services through out IT capabilities;

- Be tailored to risks and requirements that differ very significantly from country to country.

- Ensure that credible risks are addressed and that remedies for perceived risks are (i) commensurate, proportional, and well-targeted, (ii) based on a rigorous analysis of costs and benefits, (iii) are the least restrictive means, in terms of business and societal innovation, of ensuring secure networks;

- become an enabler of more dynamic and efficient markets and more open and transparent societal institutions rather a pretext for restraints on innovation and initiative in the public and private sectors

(2) Process of Developing National Cyber Security Policy

We believe that the "network model" outlined in this discussion paper can be utilized as a conceptual mechanism to help a diverse group of stakeholders to achieve a consensus view about how to approach cyber security policy.

Policymakers should focus their energies on the "drivers" that are likely to influence significantly the performance of cyber security networks — liability policy, risk management procedures and policies, market forces through procurement policies or heightening consumer expectations—and public awareness generally--about security as an integral part of IT-dependent services and products.

The unique aspects and dynamics in each country for dealing with cyber security risks need to be fully understood before new policies are implemented.

(3) Dealing with the International Dimension of National Cyber Security Policy

Government policy makers and business executives need to address the international dimensions of national cyber security policy whatever their stage of development. We believe that the network model can also be useful in helping national policy makers think more systematically about what international collaborative arrangements and resources may be required or useful.

It is important to monitor and rigorously assess how "networks" for dealing with cyber security risks are functioning and can be made more "inter-operable" on an international basis. Policy makers might usefully focus on a "node-to-node" approach to improving flows of information and collaborative relationships between national policy makers and international counterparts such as among CERTs or among firms or industry associations operating on a cross-border basis.

(4) Establishing a Minimum Set of Core Elements of an Effective National Cyber Security Policy Framework

Policy makers should focus more attention on establishing a minimum core elements of an effective national cyber security framework. These are obvious risks allowing "weak links" to develop in global networks. These weak links can create significant vulnerabilities within an inadequately protected country and on a "systematic basis" to all countries.

We believe that these minimum requirements can be achieved though a combination of policies and “process”.

There is now substantial agreement on a minimum set of core elements of a cyber security policy framework. The nine core principles embedded in the Guidelines for the Security of Information Networks of the OECD [as well as in the UN Resolution on Cyber Security] can secure as a benchmark and reference point for national policy makers in a wide circle of countries.

OECD Guidelines for the Security of Information Networks

The OECD Guidelines include, in brief:

- *awareness*—raising the visibility of risks in the public and private sectors
- *responsibility*—mandating public and private sectors stakeholders to own risks
- *response*—creating a capability to respond to incidents and threats
- *ethics*—respecting the rights and legitimate interests of other stakeholders
- *democracy*—permitting the evolution of transparent and open institutions
- *risk assessment*—capability to evaluate risks
- *security design and implementation*—factoring security into products
- *security management*—overseeing the overall framework
- *reassessment*—monitoring and evaluating progress

These principles provide a solid basis for structuring a cyber security program; and thus there seems to be no need to proliferate a new set of guidelines and principles. However, the real challenge for policy makers is to put principles into practice and to identify the specific processes and procedures that will be required to implement these principles.

The OECD has been surveying OECD countries to determine what specific initiatives are being undertaken in these and certain other countries working with the OECD. This data is very illuminating and helpful. However, we also believe that it could be very helpful to utilize the "network model" described above as policy-related tool to assess (1) the diverse experience of a broader range of countries putting in place new cyber security policies and implementing agreed principles as well as (2) explore additional options for creating a more effective cyber security framework.

We believe that it is critically important for policy-makers is to move from focusing on key principles to identifying specific practices, procedures and priorities. Principles and policy must be "operationalized". Moreover, once the focus shifts to processes and procedures, it may be easier to make cyber policy frameworks more "inter-operable" on a cross border basis as outlined above. Policy makers must commit themselves to principles as well as to a structured process of implementing those principles.

We have outlined below in Part V.C. some specific initiatives to support such a process-oriented approach.

(5) Monitoring and Evaluating the Implementation of Cyber Policy Frameworks

It is often said in business circles that what gets measured gets done. We believe that countries implementing new cyber security frameworks can usefully audit how well they are doing putting new policies and procedures in place. We believe that it should be possible to identify a number of key "audit parameters" concerning how well networks for dealing with key cyber security concerns are evolving. These parameters might include:

- The priority attached to risk management in critical industry sectors and how information flows are being managed within and among critical information industry sectors.
- The effectiveness of national CERTs in connecting with industry stakeholders and with other national policy makers.

- Flows of information among public and private sector entities; and potential blockages or required new lines of communication.
- International collaboration through the public and private sectors.
- Other key drivers of cyber networks as defined and described in the network model.

Periodic reporting and monitoring—and appropriate disclosure of the results of this process—should be implemented in a structured way to determine when and where additional technical or financial assistance might be required or warranted.[108]

Audit and assessments through other intermediaries such a multinational firms doing business in a country, security or financial rating agencies, or insurance should also be developed to strengthen external or market pressures as a tool for improving, and making more consistent, national cyber security policies.

B Some Key Recommended Perspectives for Viewing Cyber Security Policy from the Standpoint of ICT and Other Officials Concerning with Cyber Security Policy

The discussion paper sets out some key recommended perspectives on cyber security policy for ICT, other public officials, and private sector representatives to carefully consider.

These perspectives are based on the assessment we have made of the documentation and current approaches to dealing with cyber security policy around the

[108] The results of recent international surveys suggest that very few countries have developed specific metrics and benchmarks to assess the overall effectiveness of their national policies to develop a culture of security. The Danish government has developed benchmarks based on a set of common indicators (including IT security measures including virus attacks, abuse of personal information, spam, level of virus infections), IT-security counter-measures, reasons for use of IT security products. Other countries are adopting other approaches to evaluating the effectiveness of national IT initiatives. In the United States, the Computer Security Institute/Federal Bureau of Investigation (FBI) survey of cyber security is an important benchmark for assessing cyber security conditions in the private sector.

world.[109] They establish the basis for our recommendations for initiatives to create certain enabling resources set forth in Part VC.

(1) The Role of Communications Ministers and Independent Regulators in a National Cyber Security Framework

Independent regulators in various domains of responsibility – both ICT and other areas, e.g. health - and e-economy ministers may not be the lead players in a cyber security framework. However, they can have a leading role in establishing effective frameworks.

They can assist in assuring that the complexity of arrangements—and the dynamism of technological developments and risk factors—is fully and well understood by key officials with broad and important portfolios with respect to domestic and national security policy.

A cyber security policy framework has, as noted at the outset, no clear bounds or limits—geographical or jurisdictional since it necessarily encompasses, and is integral to, a full spectrum of business, societal, and governmental interests. Thus, policy makers must know how to work effectively within their span of control and responsibilities; however, they must help create a framework that is itself "seamless" and "inter-operable" in a domestic setting. In each country, public officials and business executives will have to decide how to allocate responsibilities and create specific areas of accountability but

[109] This material is included in the wiki site that we have developed in the process of preparing this discussion paper and can be found at http://www.cds-1.dartmouth.edu/tiki. We also note the OECD conducted a survey in 2003 collecting a critical mass of information and case studies on government efforts among OECD countries to implement the OECD's 2002 Security Guidelines. A report including a comprehensive inventory of national initiatives is expected to be released later this year and is likely to provide substantial guidance on "good practices" that might be followed in a wider circle of countries. We have highlighted in this section in footnotes to our recommendations a number of national initiatives that might be examined more closely by nonmember countries of the OECD. These examples are illustrative only; and the OECD report once released should be consulted for additional practices that might be of relevance and interest to particular countries.

not ignore key “linkages” of their respective areas of responsibility. ICT officials understand the dynamics of “networks” and may thus be helpful in facilitating a network-based approach to cyber security policy.

(1) *Relying on best practices:* The Swiss telecom regulatory agency Comcom has devoted considerable resources to develop a capacity to deal with cyber security issues. The FCC’s NRIC is another model for identifying telecom sector or ISP sector best practices. Information from such processes should be shared on an international basis. Other emerging cyber security initiatives developed through telecom regulators should be collected and disseminated through vehicles such as the ITU’s Global Regulatory Exchange (GREX).

(2) *Highlighting that cyber security risk factors are rapidly evolving and technologically driven:* ICT officials will need to play a leading role in identifying for other officials concerned with security policy the dynamic and technologically driven nature of potential cyber security concerns.

ICT-networks are rapidly involving. Mobile, wireless, and upcoming ad hoc network services present new challenges. Next Generation Networks will present their own new set of risk factors. New cyber risk factors such as massive sets of poorly protected systems connected to high bandwidth, phishing, spam/spim, spyware are evolving rapidly and the “black” e-economy is growing rapidly and dynamically in response to the legitimate economy. Policy responses cannot be bureaucratic in focus; they must be technologically dynamic across borders of organizations, sectors, governments, and nations.

(3) *Ensuring that main pipelines for delivery of ICT services are a first tier of an overall cyber security program:* Regulators and ICT related officials are well positioned to encourage providers of ICT backbone –

transmission and ISP services – to rely on state-of-the-art measures to minimize security risks.[110] International organizations like the ITU and the World Bank should assist in providing a wider platform for dialogue among public officials and service providers.

(4) *Ensuring that cyber security is "built-in" not "bolted on" and must be seen as an integral part of products and services from the standpoint of IT suppliers and users of such services:* ICT officials can play a leading role in convincing the public and their counterparts that cyber security must be seen as an integral part of service and product offerings rather than as an ancillary concern. This point applies, of course, to the core network infrastructure through which IT related services are provided to users in other business sectors and to government as well as to providers of ISP services. ICT officials need to make the case that what applies to the inputs to IT-related services must apply equally to "output" services and their own supply chain relationships.[111] Security levels can be improved along supply chains and trading relationships; and ICT officials are well positioned to make this case in their own immediate area of responsibility as well as with users of IT services and other public officials concerned with such services.

[110] For example, in Korea, under the Act on Telecommunications Network Usage Facilitation and Information Security, audits are performed on information security management systems in telecommunications companies and certificates are issued in order to improve the level of cyber security management.

[111] Several OECD countries are beginning to view their e-government initiatives as creating a "supply chain" relationship with their own citizens and see the initiation of e-government activities as a means of implementing cyber security controls as a condition for exchanging data with the public administration. The Austrian Government has created a Chief Information Office in the Federal Chancellery which has published a handbook on IT security practices to be followed in public authorities and businesses. This entity has required each government department to develop a security policy and to establish guidelines for dealing with external parties. See www.cio.gv.at/securenetworks/sihb/

Quality of services was brought into the main stream of business thinking about the marketing of products and services and should be an integral part of the quality management structure. The same process must occur with respect to cyber security concerns. Past experience with respect to quality of service improvements in business is an important case study for senior leaders in business, organizations, and government.

(5) *Ensuring that cyber security risk factors of business and individuals are seen as inter-related:* ICT officials as well as others need to make the case that cyber security is not only about protecting businesses and critical information infrastructure. It is equally important, even from the standpoint of overall security policy, to address the cyber security concerns of individuals.

Poorly protected PCs of individuals, when attached to high speed networks, can become dangerous instruments if and when aimed at networks and connected systems of critical infrastructures, organizations, ISPs, backbone-operators, and critical government services and functions.

(6) *Ensuring that consumers have an important part of the policy mix and must be empowered to influence policy:* ICT officials have an important role in dealing with consumers of telecom, ISP, and other ICT-related services. Though they do not have a general role in dealing with consumer protection and consumer-oriented policies, they should be well positioned to make the case more broadly to the public and in government circles that consumers have an important role to play in developing an overall cyber security framework. ICT officials should also be able to make the point to their government colleagues that public agencies are important buyers of ICT and software-related products and services.

Consumers can be empowered through awareness campaigns that will increase the likelihood that cyber safety is considered an integral part of a product or service offering. It may be useful to explore mechanisms that create economic incentives for more effective cyber security practices.

(7) *Not relying on standardization as a panacea:* Standardization alone will not be an panacea to root out network vulnerabilities; however, suppliers of services and software must be encouraged to become ever more diligent in improving the security of their offerings. Completely insulating their services and software from consumer liability through shrink wrap licensing may remove necessary market pressure for higher performance.

(8) *Developing linkages between SPAM and core cyber security concerns:* Telecom regulators in many countries have been dealing with SPAM as a significant consumer-oriented problem and burden on the national telecom infrastructure. Regulators have begun to collaborate more closely with CERTs in tracking down and addressing the sources of SPAM. Increasingly, as SPAM is becoming a vehicle for spreading BOT viruses, SPAM is being seen as a potential security risk and a bridge to the concerns of government officials concerned with the protection of critical infrastructure. In this way, the SPAM issue may be an effective vehicle for ICT-related officials to become a more integral part of efforts to establish an overall national cyber security policy framework.

(2) Role of Finance and Economy Ministers in Creating a more Favorable Environment for Risk Management on an Economy-Wide Basis

Finance or economy ministers can take the lead in creating a more favorable environment for risk management on an economy-wide basis.[112] However, they may have to do this in certain countries in tandem with ministers responsible for key industry sectors such as energy, health, or water resources. Such an environment may be created by increasing awareness of IT risk management techniques. Or it may be influenced through devices such as corporate disclosure policies or through creating roles for finance or other intermediaries such as insurance companies or "rating services".

Finance and Economy ministers should realize that firms are best positioned to know the threats they face; ministers' efforts are most profitably spent in raising the awareness of the private sector to potential external impacts of cyber events, and how entities have a shared cyber security responsibility to each other and their customers. This can be realized both through effective management of cyber security at an enterprise level as well as through the creation of a cyber security culture, where products or services are designed from the start with cyber security in mind, and customers come to expect a high standard of cyber security in the products or services they purchase. Non-market approaches such as regulation would provide incentives for firms to deal with the regulated issues and nothing more; ministers should work to encourage and empower individual players to act independently to improve the overall security environment.

(1) *Focusing on the importance of risk management in the private sector:* Developing risk management disciplines in the private sector is at an early stage even in developed economies.[113] It is the bedrock for effective cyber

[112] For example, Finland's Ministry of Finance has issued the recommendation Information Security and Management by Performance that provides principles on how to develop information security policies and management performance measurements. The text makes direct reference to the OECD principles. While developed for government institutions, the recommendations can be used by the private sector. Source: OECD materials.

[113] Approaches to encouraging better risk management in industrialized countries can vary. Some countries focus on a more centralized approach of publishing guidelines for the private sector; others focus on a more flexible approach focused on corporate governance mechanisms. For example, the German Federal Office for Information Security has developed an IT Baseline Protection initiative which includes a number of different elements. It has developed an IT Baseline Protection Manual containing standard

security policies in the future. Support for better risk management techniques requires high level attention by senior government officials and public officials. A critical component of this effort is assuring that private sector security managers understand the environment in which their firm operates, and take a very broad view of what needs to be protected. An important enabling factor is the raising of cyber security to be a board-level issue, as the board naturally takes a broad view and can bring numerous assets to bear such as consultants and audits for compliance with emerging cyber security standards such as ISO 17799.

(2) *Better understanding differences in risk management in the public and private sectors:* Private sector executives expect to deal with measurable and quantifiable risk factors and must justify security investments on a rigorous basis to financial markets. It is important to develop a good dialogue among all concerned parties about their potentially differing views and perspectives on risk management. Understanding the differences in how risk is viewed is key to understanding where there are existing incentives for private sector entities to adopt cyber security that addresses public needs, and where there is a need for intervention at a public policy level to assure security needs are addressed.

security measures for typical IT applications and systems with normal protection needs. A certification framework has developed in 2003 which has licensed 100 auditors to audit the technical and organizational implement of IT baseline protection. Finally, some IT Security Guidelines provides an overview of important security measures focusing on organizational measures and practical examples. See www.bsi.bund.de/gshb/index.htm. As noted elsewhere, similar procedures have been disseminated by the Central Information Office in Austria and the Finnish Ministry of Finance. By contrast, a number of other governments including those of the United States, Canada, Japan put more emphasis on improving risk management within the context of general corporate governance principles. In the framework of the National Cyber Security Partnership, www.cyberpartnership.org/init-governance.html, a CEO-led task force identified cyber security roles and responsibilities within the corporate management structure. To promote information security governance within corporate management, the Japanese Ministry of Economy, Trade, and Industry (METI), set up the Committee on Information Security Governance in September 2004.

(3) *Relying on informal as well as formal collaborative mechanisms in developing risk assessment networks*: The focus should not only be on creating new structures and institutions. Informal cooperation at all levels should be encouraged using web-based capabilities and direct contacts. Intermediaries such as insurance companies or IT safety rating agencies may be used to improve the level of risk management in the private sector. For example, the Common Vulnerability Scoring System (CVSS), is a vulnerability rating system developed by the US National Information Security Council (NIAC). The ambition of NIAC is to provide open and universal security ratings of software vulnerabilities.[114] The advantages offered by the adoption of vulnerability scoring system include global visibility, a common understanding of how the system works and increased possibilities for support of IT vendors and community worldwide.[115]

Establishing a rating scheme may begin to provide a benchmark against which potential investors can more objectively evaluate decisions to invest or expand their operations in other countries.

(3) The Role of Security Coordinating Mechanisms: Making Complex Security-Related Networks Work

In dealing with new challenges of managing complex security-related networks, a number of key principles are relevant. Piece meal approaches to cyber security do not work. Novel initiatives may not be required. Existing policy tools and procedures can be

[114] The framework is in its first-generation stage and still needs to be tested. In 2005 it was decided that this feedback would initially be provided by a Special Interest Group within FIRST, the Forum for Incident Response and Security Teams. The lack of a common scoring system led security teams worldwide solving the same problems with little or no coordination. In addition the internet and its vulnerabilities do not belong to one country, and therefore any technology that is to be adopted globally must have technical merit and the support of an internationally recognized, non-governmental organization.

[115] 115 http://www.first.org/cvss/

used more effectively.

(1) *Conducting an overall review of national cyber security policy:* A national policy coordinator might usefully initiate a base line review of national cyber security policy. Such a review would involve convening all key stakeholders and formulating an overall approach to national cyber security policy along the lines outlined in Part V.A.1 above. This review would assess and define the respective roles of all key stakeholders.[116] It might assess the practical utility of analyzing national policies in light of network model as described in this discussion paper.

The baseline review would be conducted as well with an expectation that cyber security policy would be reviewed and audited on a periodic basis both by national as well as international observers and experts from either public or private institutions. This review process should also be structured to ensure the joint participation of the security coordination agency as well as representatives from the ICT sector.

(2) *Education, human resources concerns and development must be given high priority:* One key element of effective cyber security policy must be creating the right awareness of and incentives for cyber risk management at all levels, from national to town governments, from large corporations to small businesses as well as home computer users. This should take the form of multi-disciplinary, comprehensive educational initiatives,

[116] The Australian Government has evolved a well-structured framework for focusing the resources of the public and private sectors on cyber security concerns. This framework provides a useful benchmark to take into account in any overall review of national cyber policy arrangements. The Australian Trusted Information Sharing Network (TISN) (www.tisn.gov.au) was launched in 2003 and enables owners and operators of critical infrastructure to share information and develop strategies to mitigate risk. TISN comprises the Critical Infrastructure Advisory Council, a number of Infrastructure Assurance Advisory Groups (IAAGs), and a number of expert advisory groups.

including encouraging the enculturation of cyber security best practices in technical practices, promoting risk management practices in business settings, and "public health" type educational initiatives (e.g. "safe surfing") for the general public.

The short term element is awareness raising for identified target groups (e.g., small and medium-scale enterprises, the general public), and the education of the do's and don'ts at schools and for other groups in society.

Another element to consider is to include cyber security as a main element in the curricula of courses up to and including the university level education of ICT-professionals (as programmers, system and network management). Finally, a full scale cyber security education structure could be created to educate cyber security professionals (e.g., teachers, cyber security officers, cyber security researchers).

(3) *Basic software and network services need higher levels of quality which may be achieved through use of the government procurement policy:* Procurement policy can be utilized to influence the priority attached by IT network and service providers. Buying decisions can be concerted on an inter-agency basis as well as through collaboration at the regional or international level.[117] International organizations might well consider whether they might raise the priority attached to security-related concerns in connection with their core advisory activities.

[117] See, for example, the Common Criteria Mutual Recognition Agreement which provides for mutual recognition of certificates issued by national certification bodies for measuring the trustworthiness of IT security products and systems using the "Common Criteria" ISO/IEC 15408 standard. In November 2003 the signatory countries to the agreement were Australia, Canada, France, Germany, Japan, New Zealand, the U.K., the U.S., Spain, Austria, Finland, Greece, Hungary, Israel, Italy, Norway, the Netherlands, Sweden, and Turkey. See http://www.commoncriteriaportal.org/.

(4) *Mobilizing public "outreach" and more effective communication to the public and private sector:* Cyber security risk factors and threats are complex in nature as are the necessary policy responses. Vision, leadership, and more effective communication by business leaders and public officials are critically important. One of the consequences of outreach initiatives may be to enhance the role of consumers of telecom and ISP services and market forces in influencing the attention accorded to cyber security concerns.[118]

(5) *Best or good practice information needs to be more widely disseminated:* Wheels do not have to be reinvented. Effective practice can be shared using web-based resources. The focus should not be exclusively on identifying "best practices". The effort should catalogue "good practices". Government procurement policy should be used as a tool for improving the overall level of cyber security protections. Further inquiry should be undertaken into the dynamics of third partner intermediaries that might more effectively use market-related pressures to improve security performance.

(6) *Assessing potential threats more effectively:* It is difficult to mobilize new resources and financial support on the basis of hypothetical threats and poorly documented assessments of risk factors. Public agencies need to

[118] Examples of a diverse array of outreach efforts have been well documented through recent international surveys. This diversity of international experience, when made publicly available through the publication of the results of the OECD survey of national initiatives to implement the OECD Guidelines, will be very useful to developing countries seeking to implement an integrated and comprehensive effort to raise awareness of cyber security issues. A number of countries have designated a National Information Security Day; others have relied on industry associations or other ad hoc groups to raise national awareness of cyber security issues. An industry association in the United States, the National Cyber Security Alliance, has focused on best practices in education and awareness and made suggestions for how a public/private national outreach awareness campaign could reach 50 million home users and small businesses in one year, using paid and unpaid media, ISPs, security vendors, and other outlets. See http://www.cyberpartnership.org/init-aware-html.

add their credibility to a joint effort by public and private sectors to assemble on a more integrated view of potential threats and its dynamics. This requires more effective cooperation among CERTs, ICT-related ministries and intelligence agencies both in a national and international context.

These threats must be realistically appraised and addressed in a proportional and measured way. They must be weighed in light of the stage of economic development and vulnerabilities of each country.

(7) *Focusing on shifting and reallocating responsibility and liability as a policy tool:* In the view of some observers, security levels can be significantly improved through clarifying responsibility of service providers through imposing liability for inadequate safeguards and preventive measures. However, telecom and Internet service providers claim that they are bit transport operators not focused on the content of information conveyed. This viewpoint is sometimes based upon the local difference in telecommunication (bit stream) versus IT-laws (content). Taking any responsibility for content rather than the bit stream may cause much more law enforcement investigation calls and related costs. Shifting liability may be a risky option as and if governments step in and start asking for all types of analysis of information conveyed, e.g. porno, data-mining on money-transfers. It is important for service providers to stay independent. At the same time, inadequate corporate disclosure of cyber risk factors can also be a basis for corporate liability and may create an incentive for more effective risk management.

Policy makers must carefully evaluate whether and when increased liability can produce counter-productive consequences. Using liability as a policy tool can have many unwanted consequences imposing disproportionate burdens and costs on business. In many countries, reliance on litigation is not consistent with custom and practice and legal traditions and is unlikely to be an effective policy tool.

(4) Role of Agencies with Responsibility for Intelligence, National Security and Law Enforcement

Intelligence, national security, interior, or justice ministers all have critical roles to play in an overall cyber security policy framework. One key challenge is building bridges among intelligence and security services and the sector ministries that may be more directly and critically involved in managing cyber risks.

Flows of information from intelligence and security services to private sector entities responsible for critical information infrastructure is another area requiring close attention.

As discussed above in the discussion paper, there are likely to be significant discontinuities in approach among countries where security services have historically had a dominant role in security-related matters and those where cyber security issues may be led by agencies clustered around CERTs or IT Ministries in a more open "networked" configuration.

Building bridges between these different frameworks is likely to be a very demanding aspect of improving the inter-operability of national cyber security networks. Cyber exercise may be one useful policy tool to address these concerns.

(5) Role of International Affairs Agencies:

Current arrangements are still too nationally oriented notwithstanding the importance international undertakings of the European Commission, the Council of Europe, the OECD, and the G8. International associations or confederations of industry, sectors (e.g., the ITU and its various study groups, the UCTE), international bank associations, SWIFT) are starting to understand the urgency to increase the protection of CII. These organization, when addressed in the right way, are able to push internationally harmonized protection standards which their members can take up, e.g. the BASIL II standards.

International organizations might usefully focus their energies on improving capacity building mechanisms available to countries that involved in high level nationally or regionally-driven initiatives to improve cyber security protection. In Part V.C, we have outlined a number of initiatives to strengthen national capabilities through developing mechanisms for information sharing, collaborative research and policy-related activities, training, and exchange of practical experience and know-how.]

(6) Role of the Private Sector Stakeholders

Cyber security is at its core a shared responsibility. As the owners and operators of most all of the ICT and critical infrastructures, private sector entities play a central role in cyber security. We offer some suggestions as to how private entities can better assume their responsibilities (for research examining what motivates firms to adopt higher levels of cyber security, see Appendix A):

(1) *Ensuring firms take a wide view of the risks they face.* Firms whose manager of security adopts a very narrow view of what needs to be protected will adopt a level of information security that is ultimately insufficient for both their own and the public good. Firms need to understand how the disruption of their ICT-mediated activities would affect them, and their business partners and customers. This broad view will result in a more appropriate level of cyber security for the firm and the public.

(2) *Addressing cyber security as a board-level issue.* Raising cyber security to the level of the board of directors sends the message that cyber security is a serious topic. The board will have a wider view of the firm’s place in the economy—and its various strategic relationships with its competitors and collaborators and with the public sector--and will be able to ask the

questions of how cyber incidents will affect the firm's ability to operate. The board should require that the firm prepare for the board periodic reports concerning its cyber security risk profile and how the firm's cyber security mechanisms match current best practices. It should keep abreast of, and conform with emerging best practices with respect to IT corporate governance.

(3) *Being proactive in addressing risk by qualifying business partners and collaborators.* There are many types of risk that a firm faces, but has limited control over. Examples include the protection of corporate data held by others, and the cyber security policies of critical business partners. Firms should start placing responsibility for vulnerabilities with those entities that are best positioned to manage the vulnerability: if a supplier is holding data, the firm should take steps to assure that the supplier is holding the data in a secure manner. By qualifying potential suppliers in this manner, firms are both reducing their risk, and are raising the general level of cyber security. Firms should evaluate the full range of their various contractual relationships both with intra-corporate entities as well as with external suppliers of various types, distributors, and other business partners and collaborators. They can then focus on measures to improve cyber security over these "networks" of corporate relationships. In this way, through key points of intervention and initiatives by "driving players" in supply chain relationships, the scope and effectiveness of "cyber security networks" can be increased.

(4) *Developing firms' relationships with their peers, and then sharing information with their peers.* Education about cyber security will be an ongoing process for some time, and the best way to learn about the current threats and how to deal with them is through working with others who are in the same environment, facing the same issues. These groups should be

informal in nature, as opposed to the formal sharing that takes place in ISACs.

C Initiatives to Develop Enabling Resources for the Development of the International Cyber Security Policy Framework

Many multinational organizations including the ITU, the World Bank, the European Union, have an interest and mandate to deal with some, but not all, aspects of the multi-dimensional and complex aspects of cyber security concerns. It may be important for these organizations to focus on how they can work, together in collaboration with private sector stakeholders, to create new venues for international collaboration.

These venues may not need to be structured as part of a administrative division or committee of an established organization. Nor is it likely to be necessary or desirable to create a new specialized agency. Instead, it may be preferable to encourage a diverse group of stakeholders including research institutes and education institutions to create an ad hoc collaborative structure for sharing experience, information, or conducting common undertaking such as cyber exercises.

It is not enough to focus on the most important national economies and the most critical economic sectors. Because of the potential threat represented by BOT networks, poorly safeguarded national ICT-markets can become a haven for groups that might pose a threat to critical information sectors either in these same vulnerable markets or in other countries.

Since as noted elsewhere cyber concerns cannot be easily categorized and compartmentalized on a jurisdictional or geographic basis, there may be much to be said for creating an ad hoc institutional space that does not require the creation of a new international organization or rely on an existing division or committee of any particular international organization. Such an ad hoc approach would be quite consistent with the mandate arising from the first session of the WSIS which advocates "a mechanism for the full and active participation of governments, the private sector and civil society from both developing and developed countries…”. See Declaration of Principles and Plan of Action, Geneva Plan of Action, C.6, World Summit on the Information Society, Geneva, December 10-12, 2003.

(1) *Developing collaborative structures for policy research:* Common research capabilities can be developed through a collaborative model. There are many models to choose from including the i3p model in the U.S. and the European common research initiatives. Collaboration might occur at different levels through the identification of common research priorities.

In addition, it is apparent that the role of ICT-related agencies in cyber security policy is likely to increase. There are existing collaborative consortium of experienced international telecom policy research institutes (such as ENCIP) that have to date had a limited role in dealing with cyber security issues. However, these constitute an important contribution in the future directly and through their own networks of collaborating institutes in developing countries.

(2) *Creating a collaborative undertaking to update and share cyber security related information and documentation:* Other activities such as collection of country experience and developing case studies and best practice might be developed collaboratively through wiki-based capabilities. The current data base collected in this project could be turned into a shared resource.

(3) *Developing more effective inter-disciplinary collaboration among institutes and research centers documenting institutional structures and policies and those dealing with the economic and dynamic aspects of cyber networks*: With a data base keyed to network model, information and assessments could be collected on a country specific basis to validate and test the hypothesis that a network model can be a useful way to

improve understanding about how cyber security issues are dealt with in different countries. Institutes like the Swiss Institute of Technology, ETHZ, could be a useful contributor to this international collaborative model along with business school and government and non-government-affiliated research institutes. It may be very useful, for example, to look more closely at, and undertake case studies relating to, IT-related corporate governance mechanisms –and the oversight of “supply chain relationships” in the broad context outlined in V.B.6 (3) herein—in a variety of different national context, The focus might be on such mechanisms in entirely state-owned enterprises or such state-woned enterprises that are in the process of being restructured through an infusion of private capital.

(4) *Collecting and collating statistical data concerning cyber threats and incidents:* Data on the level and profile of cyber threats in emerging markets is not readily available and collated on a regional or international basis. An international research consortium could play a useful role in stimulating the development of metrics for monitoring the cyber security “weather” in different countries and regions around the world. A cyber security “meteorology service” –that provides information that is more visible and transparent than that offered by private firm specialists in this area with an interest in maintaining the exclusivity and economic value of their data—could play a beneficial role in creating greater public awareness of cyber security concerns and in building out the intricate and multi-tiered web of networked relationships described in this discussion paper.

(5) *Focusing international collaboration around other issues of immediate strategic importance such as SCADA systems:* Research on important sector specific topics related to SCADA systems should be conducted on a

multilateral basis as it is being undertaken. Significant research and policy assessment is being undertaken on a parallel basis in the United States and in the European Union relating to SCADA systems. These undertakings could, and should, be interlinked and related as well to potential research and policy-related centers in developing countries. A portal or other forum for sharing research and exchange of ideas should be developed. In addition, the sector groups in international development banks concerned with infrastructure and utility distribution systems should be more directly linked into emerging research activities.

(6) *Exercises should be used as a critical tool for developing and refining "new collaborative networks":* Exercises should be developed as a device for establishing new "neural paths" and "connecting links" among key participants in international collaborative networks. It is likely to be an important mechanism to bridge over differences in institutional approaches. See Part IV above. Exercises have been utilized on a regional basis for emergency contingency planning or other scenarios involving the impact of terror events by a range of international organizations including those with national security roles such as NATO.

A common resource regarding exercises should be developed that permits sharing of experience where possible or feasible within security-related constraints. Technical assistance from such sources of exercise development should be developed on a more inclusive international basis.

It may be useful to consider whether an "exercise in a box" capability could be developed.

(7) *Coordination of cyber security activities and best practices among universities on an international basis:* Many universities are recognizing the importance of increasing the level of security of their often loosely

coordinated processing centers and data bases. Often such university systems represent significant clusters of very substantial bandwidth and computer processing power that may represent a significant target for hackers, or even a potential external security threat, if such processing capabilities were directed at unprotected critical information infrastructure.

A collaborative exercise in sharing best practices might have significant spill-over benefits in terms of raising the overall level of cyber security protection in a national context.

(8) *Consultations need to be improved through web-based conferencing:* It is important to develop better tools for bringing experts together on a virtual basis. The medium of virtual conferencing needs to be developed through practical steps and experience with information exchange among research institutes and policy makers.

The World Bank has encouraged in recent years the development of a Global Distance Learning Network. This network consists of a world-wide group of video conferencing centers that are locally managed and control. To date, these facilities have been largely used for more traditional training and educational activities. However, building awareness and capabilities to manage complex cyber networks may require much more peer-to-peer exchange of relevant experience. In addition, at each level of national network relationships there may be opportunities for exchange of views among counterparts. Virtual networking could also provide a platform for table top “mapping exercises” described elsewhere, especially in Part III.

Appendix A Case Study of a U.S. multinational firm and selected suppliers

Information Security in the Extended Enterprise: Some Initial Results From a Field Study of an Industrial Firm

Abstract

What are the main drivers of private-section investment in information security? How exposed are firms to cyber risks arising from their reliance on the information infrastructure? Initial results are presented from a field study of a manufacturing company and four of its suppliers of different sizes. We find that many managers believe: that information security is less a competitive advantage than a qualifier for doing business; that firms' internal networks are not at additional risk as a result of using the information infrastructure to integrate their supply chains; and that their supply chains are robust to internet outages of up to a week in duration. We discuss their security perceptions and actions in the context of a cost model.

Introduction

As organizations increasingly rely on the internet for their internal and external business processes, each firm's security decisions have an impact on the overall security of the information infrastructure for the thousands of suppliers, collaborators, and channel partners that they interact with as part of that firm's extended enterprise (a collection of firms that design, produce, and market a product or service [Dav2004]).

Each firm in the extended enterprise must have access to critical business information such as product specifications, marketing plans, and vast transactional data on product sales and movement within the supply chain. Managing the security of this sensitive information flowing across the extended enterprise is a significant and under-researched topic. Firms often make information security decisions with very limited information about the threats their systems face, the strength of their systems against these threats, and the efficacy of additional security measures. Outsourcing and globalization present even more difficult security issues; in many industries competition is quickly changing from firm against firm to extended enterprise against extended enterprise.

Understanding the economics of information security within and across firms will necessitate understanding the process by which firms adopt information security mechanisms; this will expose existing drivers and possible incentives promoting greater information infrastructure security. Separately, understanding the risks referred across the extended enterprise is critical to defining a level of information security to minimize those risks, and is a step towards developing a business case for the security needs of the firm as well as addressing what level of security is needed for the greater public good. Understanding these issues will enable policy-makers to make reasoned decisions regarding what policies might be needed for and what policy mechanisms will be effective at promoting an increased level of security in the information infrastructure.

Over time, to the extent the business case is understood, the market might drive enhanced security and help close vulnerabilities, addressing some aspects of current market failures. As a policy matter, serious research into these issues will allow chief executive officers (CEOs) to talk with their peers and government leaders about this issue from a fact-based and theoretically sound foundation and enable CEOs to add significantly to sound policy-making.

While there are a few papers that have studied return-on-investment (ROI) on information technology (IT) security investments at the firm level ([Bla2001], [Gee2001], [Gor2002], [Soo2001]), little empirical work has been done at the firm level to understand the processes involved in information security. Like the interdependent security risks faced by other business partnerships ([Gun2004], [Kun2002], [Kun2004]), such as baggage handling in the commercial airlines, we hypothesize that information security risks across trading partners exhibit many important risk management challenges.

We have identified three research efforts that address the core information security issues pertaining to the efficacy of economic and other potential drivers of information security, the risks to which critical business infrastructures (supply chains) are being exposed, and to what extent security decisions need to be made with an eye to managing risks beyond one's local organization. These research efforts are:

- To understand how firms adopt information security capabilities. How do firms currently make security investment decisions? What are the key drivers? A key objective is understanding the drivers that influence firm's information security investment strategies.
- To access interdependency risk magnitude. How large is the real or perceived security problem for the extended enterprise? What are the security risks and how do those risks translate into business risks? Knowing how vulnerable or resilient supply chains and extended enterprises are to security failures of one of their members will directly inform the policy debate about how much information security is needed for the greater public good.
- To evaluate the information security gap. Are larger companies only as secure as their least-secure supplier? Are larger firms making better security investments (and better patch management decisions) than smaller firms, creating a security gap in the extended enterprise, which may render all interdependent companies as vulnerable as the weakest critical company in their extended enterprise [Joh2004]? Is anyone managing the risk across the extended enterprise? Should large, relatively secure firms be concerned about collaborating with smaller, less secure firms?

This paper presents initial results of a study that explores these questions through field research of firms of different sizes and their supply chains. The results presented relate to the first two points of interest described above.

Methods

The field study consists of a set of interviews with security and supply chain executives and managers at a "Host" firm and four of its direct suppliers (direct meaning that the supplier's product is core to the product of the Host). The interviews were designed to elicit the knowledge and beliefs of the interviewed individuals; security audits of the interviewed firms were not a part of this study. Thus, the results of this study reflect the beliefs of the interviewees without an external check on the validity of certain statements (like the recent AOL/NCSA Online Safety Study [AOL04]). By asking the same questions of different interviewees in the same organization, we were able to look at the internal consistency of information provided in interviews.

The Host firm is a Fortune 500 manufacturing firm with plants and sales worldwide. A series of interviews were conducted with security, information and supply chain executives and managers at both the headquarters level as well as at an individual business unit (BU) level. In all, 13 individuals were interviewed. Interviews were based on a set of questions and conceptual frameworks designed to gain insight into the issues under study for each particular role interviewed. Interviews were conducted in person with one or two researchers, and one to four interviewees. Interviews lasted from 30 minutes to 2 hours. At the start of each interview it was made clear to the interviewees that the interview was anonymous; during the interview every effort was made to build a high degree of trust with the interviewee. Host interviews were conducted July 2004 through February 2005.

As this set of interviews was designed to be the first in a larger study, this study was treated as a pilot study in that the set of questions asked during each interview changed. Specifically, a set of role-dependent core set of questions was asked at each interview; as the series of interviews progressed, additional questions were introduced in an effort to deepen the understanding of the research issues.

With the aid of the Host firm, six candidate supplier participants were selected. These candidates were chosen without regard to their information security capabilities; we had no knowledge of their abilities or their history with the Host firm in that regard. The criteria used to choose the candidates were:

- Candidates had to use some form of electronic communication to manage their supply relation with the Host. This was a requirement.
- Candidates would be a range of sizes in terms of their annual revenue. This was a requirement.
- Candidates would provide products directly used in the Host's products. This was a requirement.
- Candidates should be close to a small set of geographic locations. This was a nice-to-have.

The Host asked the candidates if they were willing to participate in the study. Five of the six suppliers contacted by the Host agreed to participate in the study; of these five, four were interviewed. At the suppliers we spoke with information security and IT executives and managers, and where applicable the account managers of the Host's account. For the four suppliers, nine individuals were interviewed. Supplier interviews consisted of one researcher and 1-2 interviewees. Four interviews were conducted in person; the rest were conducted by telephone. Supplier interviews were conducted December 2004 through February 2005.

In terms of exploring how firms made information security investment decisions, the interview questions were the same as those used for the Host interviews. With regards to the risks developed through supply chain integration, while the original intent was to ask questions only about the Host-Supplier relationship, the discussion at the host and supplier firms covered both supplier and customer relationships for that firm. As with the Host interviews every effort was made to establish a high level of trust with the interviewee. At the start of the interview, it was made very clear that the interview was anonymous, and that the purpose of the interview was informational and not in any way an audit of the supplier's information security capabilities.

Results

We were able to develop a host relationship with a Fortune 500 manufacturing company; the results we present here result from interviews with 13 executives and managers of IT, information security and supply chain at the Host, and with 9 executives and managers of IT and customer accounts at 4 suppliers to the Host. Table 1 gives some particulars about the Host and the suppliers.

	Product	Number of locations	Annual Revenues	Subsidiary?
Host	Conglomerate	many	several billions	No
Supplier A	Metal	many	few billion	Yes
Supplier B	Logistics Services	many	few 100 millions	Yes
Supplier C	Printing/Design	few	few 10 millions	Yes
Supplier D	Metal parts	one	few millions	Yes

Table 1: Properties of Interviewed Firms.

1. Drivers of Adoption of Information Security

While each firm approaches information security in a different manner, there are some patterns that emerge. InfoSec managers talked about the set of processes that were used to arrive at their existing level of information security in much more nebulous terms than they talked about the drivers of the adoption of additional levels of information security.

First, the primary driver of firm's existing level of information security is the InfoSec manager protecting their firm's internal network and data. The process of how InfoSec managers arrive at their current level of information security was not well-described, likely because it was not the result of an external dialogue, but of a dialogue internal to the InfoSec manager. For deciding on this base level of InfoSec, InfoSec managers use their past experiences, the experiences of trusted colleagues, consultants, trade magazines, web research and other mass media.

While the resulting baseline InfoSec practices differ by company, the results are reported as being the same across all interviewed firms: none has experienced a virus, worm, break-in or web defacement in the last year.

Second, the main drivers for the adoption of additional information security are government regulation and customer requirements. While more than one firm talked about Sarbanes-Oxley as shining a spotlight on their internal information security procedures, none said that their level of information security increased as a result of Sarbanes-Oxley.

With one exception, firms had an analogous reaction to customer requests for information security. Every firm interviewed described itself as being responsive to customer requirements for information security; one supplier said that customer requirements would be the big driver of further information security efforts. Within this set of firms, customer demands have mainly come in the form of questionnaires, some of which were quite extensive. Industries that have presented these questionnaires include aerospace, oil, and trucking. The interviewed firms view these questionnaires as representing a qualification for business; with the probable exception of Supplier D, these questionnaires did not affect the level of information security at the firms as the firms already had sufficient information security.

As a group, the interviewed firms made few or no demands on their suppliers for levels of information security, although Supplier B said that they would start having requirements in the near future.

Of the five firms interviewed, four think of information security as a cost and a qualifier. The director of IT at Supplier B thought that information security was a competitive advantage in the sense that customers felt more comfortable in doing business with them as a result of their focus on information security. With this exception, nobody interviewed thought that information security would ever become a competitive advantage.

2. Risks to Extended Enterprises From Reliance on the Information Infrastructure

Two types of risks were explored in detail: risks to internal IT systems and information as a result of integrating the supply chain using the information infrastructure, and risks to a firm's ability to produce product as a result of supply chain disruptions caused by information infrastructure events.

Information Security Risks

The great majority of the internet-mediated communications the interviewed firms have with their customers and suppliers is via email and web-based applications.

The Host firm communicates with its suppliers using Electronic Data Interchange (EDI, essentially a standardized, codified email format for communicating information about orders), a database-backed web application, a few virtual private network (VPN) connections that are isolated to the server hosting the required application, and email. The security manager at the Host regards web-based applications as the type of connection carrying the highest risk to the Host's internal network, with VPN being second, and EDI and email third.

Of the suppliers, A and B used EDI and email to communicate with their business partners (customers and supply chain), and did not utilize VPN or web-based applications. Supplier C used only email; D used email with a single supplier having access to information stored in a database using a web-based interface.

	Web App	VPN	Electronic Data Interchange	Email
Host	Y	Few	Y	Y
Supplier A	N	N	N	Y
Supplier B	N	N	Y	Y
Supplier C	N	N	N	Y
Supplier D	Y	N	N	Y

Table 2: Types of Connections Firms Utilize with Their Business Partners

None of the firms interviewed had experienced a compromise of security to their internal systems as a result of their electronic integration with their suppliers.

Risks to Supply Chain Continuity

What are the risks to the Host's supply continuity as a result of using the information infrastructure? These discussions were framed around the case of the Host losing the ability to communicate with suppliers via the internet for various periods of time. All firms interviewed said they would use phone, fax and FedEx to communicate with suppliers and customers in cases of prolonged internet outage; none thought that such an occurrence would result in any lost business.

To understand the level of disruption an internet outage would have on the supply chain of the interviewed firms, an effort was made to understand how the various firms communicated with their supply chain. The results are summarized in Table 3, which shows the division of the types of communications used to order their supplies at the time of the interview.

The business units (BUs) and divisions interviewed at the Host are the largest user of the internet for supply chain management; the use of web applications and EDI accounted for over 3/4 of the orders sent to all suppliers of these BUs and divisions. Executives at each BU said that it is their goal to move 100% of their suppliers to use either a web application or EDI in the near term.

Supplier A, a multi-billion dollar company, uses only phone and fax to order their supplies. Supplier B relies on EDI for 60% of its supply chain communications with the remainder being phone or fax. Supplier C uses email to order 80% of their supplies; they follow up both their email and fax orders with hard copies sent by mail.

	Web App	EDI	email	Phone/Fax
Host BU #1	88% of PO’s online		0%	12%
Host BU #2	~77% of PO’s online		0%	~23%
Supplier A	0%	0%	0%	100%
Supplier B	0%	60%	0%	40%
Supplier C	0%	0%	80%	20%
Supplier D	0%	?	?	?

Table 3: Percentage of Interviewed Firm’s Supply Chain Order Communication by Connection Type

Despite its dependence on the internet for communication with its suppliers, Host interviewees noted that the worst thing that could happen from a supply chain perspective would be for the Host’s intranet to go down; this would directly affect plant’s abilities to access the Host’s internal inter-plant ordering system[119], resource planning systems, and other automated systems supporting the generation and processing of orders. The Host has invested in a backup ISDN system with the intent that all the Host’s locations would be able to communicate with each other if the internet were to fail. Supplier B also has invested in a frame-relay backup system that is completely separate from the internet; this would link all their sites.

From the standpoint of the suppliers and supply chain continuity, the impact of lack of access to the internet is mainly time-dependent: the longer the outage, the greater the effect. Table 4 combines the reported impact that outages of various durations would have on the supply chains of the interviewed firms.

There were several viewpoints expressed during interviews at the Host, including the impact of security on both their supply chain and their participation in the supply

[119] At the Host, the largest suppliers to some plants are other Host plants.

chain of their customers. The shortest interruptions that would be noticed were surprisingly short, on the order of 15 minutes. This is due to a requirement of some of the Host's customers that they be notified within 15 minutes of the Host shipping product to the customer; failure to send this advance shipping notice (ASN) is noticed, and is a factor in renewing a supplier's contract. Some executive at the Host were more concerned with the potential impact of short outages than those of longer outages.

As the length of an outage increased, Host interviewees talked about additional variables that affected how an internet failure would impact the Host's business continuity. The overall sense was that the Host would do whatever it took to maintain the ability to produce and ship product; they felt that the element that would suffer most would be invoicing and payment; that would be secondary to the actual ordering of supplies and production of product. When the conversation moved beyond this generality, interviewees talked in greater detail about other factors that would impact the Host.

One interviewee talked about plant volume. The Host has high-volume plants that

Internet down for:	An afternoon	1 day	3 days	A week
A Host BU #1	No impact	Low volume plants: supply-side pain	Hi volume plants OK	Hi volume plants: shipping issues
Host BU #2	ASN disruptions - impacts customer	Stock available for production	Customers would see slack	Unable to produce all items
Supplier A	No impact	No impact on supply side; "big deal" on customer side		
Supplier B	[confident there would be no impact on supply or delivery of products]			
Supplier C	No impact	No impact	No impact	No impact
Supplier D	No impact	No impact	No impact	No impact

Table 4. Reported impact of an Internet outage of various durations on the supply chains and customers of interviewed entities.

produce substantial quantities of the same product, and other plants that produce small numbers of customized products. From a supply-chain perspective, the high-volume plants would be able to sustain a 2-3 day internet outage without difficulty; this interviewee expected that around that point the suppliers would start calling the Host; there would be no need for the Host to call the suppliers. He termed this “supply chain learned behavior”, and noted that for high-volume plants there is a lot of forecasting information shared between the Host and suppliers, so the suppliers have a good idea of the Host’s needs for a substantial amount of time. He thought that if internet connectivity were out for a week, the supply chain would be operating, but the finished products would be piling up on the shipping dock due to the impact of the outage on the Host’s ability to interact with its customers and shippers.

Another Host interviewee echoed this theme, noting that the amount of disruption caused within the supply chain is dependent on the number of customers a supplier has: if a high-volume plant ships to only a few customers (think of large potato growers who supply McDonald’s: they only have one customer), it is possible to process orders sent by phone or fax. Such relationships would also be involved in forecasting. If the same plant were to have to take orders by fax or phone from thousands of smaller firms, it would be very challenging.

In contrast, the low-volume, custom plants would be affected to a greater extent by an outage. In the example he was using, the custom product requires components with lead times of days; in order for a part to be available to be integrated into the product in a timely fashion, it would have to be ordered today.

Supplier A said that there would be not impact to their supply chain as a result of an outage of the internet, as all their supply chain communications occur via phone or fax.

While EDI was a very significant part of Supplier B’s communications with its supply chain, the interviewees felt that there would be very little impact if they were unable to access then internet. Supplier B felt the biggest impact would be on invoicing and payment.

Supplier C, the printing and graphics design firm, was confident that an internet outage would not affect either their supply chain or their ability to produce product for their customers. In explaining their supply process, it came out that even when they use email for ordering, the email is essentially a follow-up of a phone call; the email is followed up with a print-out that is mailed to the vendor. They feel the volumes of supplies ordered is small enough such that they would be easily be able to manage their supply and direct customer needs with phone, fax and FedEx.

Supplier C thought the largest impact would be in maintaining their customer relations; they like to maintain a close relationship with their customers using email. An internet outage would greatly affect this.

Discussion

Drivers of Information Security

The cyber security issue is both an economic and a technology issue. The technologies within the enterprise, between enterprises, and across the internet, all sit in markets. Therefore, the issue of vulnerabilities throughout the system sits within the context of the existing market structure and the various technical, competitive, policy and legal factors.

This market is often thought of as being a classic “public goods” market – that is, that the market under current conditions leaves a certain amount of economic welfare unaddressed, and that loss of welfare is defined as a market failure. In this market, we may pay for security on our own systems, although there is evidence that we do not know exactly what the cost-benefit analysis is, but we may not pay to protect others who connect with us or the internet – those are “externalities” (things that happen to other people) that we won’t easily internalize. As the issue sits in the market place now, we know that there are vulnerabilities throughout our networks of networks.

In the face of market failures impacting the economy or the national security, there are traditionally two approaches: private and public. Private approaches can include new business models that change the market, innovation, the effects of increased transparency and information, voluntary standard setting, ”good practices”, contracts between parties, insurance, corporate good citizenship, and the like. Public responses can include changes in research and development funding, liability, regulation, mandatory standards, tax policy, government procurement and standards, and the numerous other ideas that have been discussed by the government.

In this context, Freeman [Fre2004] argued that there are four classes of drivers for increased information security: market forces, government regulation, government spending, and litigation. Do our results provide any insight into the effectiveness of these drivers?

Government Regulation

The interviewed firms certainly pay attention to government regulation; ‘government regulations’ was mentioned more than once as one of the top three information security drivers. While they might pay attention, in general they do not think that government regulation would be the best manner for promoting effective information security, a view shared by others [Dyn2004]. More than one of the study participants had recently completed a Sarbanes-Oxley audit. Sarbanes-Oxley, while not specifically about information security, has some impact on firm’s information security practices. While one of the interviewees felt that Sarbanes-Oxley improved their information security, he also said that he thought the effect of Sarbanes-Oxley was to move the focus of attention from important security issues to less-important issues.

Market Forces

Every firm will adopt some level of information security, either deliberately or through neglect. In a 2002 paper, Gordon and Loeb developed a model to explain the optimal level of investment in information security. Here we embrace and complement their model to provide a context in which to understand our results. These authors argue that the optimum level of cyber-security investment is where the marginal costs of increased information security equal the marginal decrease in the costs due to events such as virus attacks, hacking, break-ins, etc. As written, these arguments represent a definition of the optimal level of investment in information security for the organization's good. Implicit in this optimal level is a definition of what is being protected; the optimal level of investment will likely differ if a firm is trying to protect their internal IT infrastructure, or their external dependence on the information infrastructure. We label the level of information security investment optimal for their local good (their internal IT-systems) as O_L in Figure 1.

For any firm, there is a level of information security investment that is adopted; we will call this the security baseline β. This level reflects decisions made within the firm

Top concerns of security managers:	
External break-ins Internal information Business continuity Disaster recovery InfoSec posture of vendors	Internal employees Process security (do applications behave as expected?) Redundancy Spyware
Practically of no concern:	
Infosec posture of vendors Data corruption Data obfuscation Insider attacks Internal systems	

Table 5: Information security manager's reactions to selected security issues. The numbers in parentheses indicate the number of respondents reacting to the issue.

about what they are protecting: some firms may take a very local view and only think of their internal IT infrastructure; others will take a more global view and also think about

business processes linking them with their extended enterprise. As drawn in Figure 1, β is to the right of O_L, reflecting our belief that some of the interviewed firms were investing in security at a level greater than that required for the local optimum. This belief is based on the fact that they could identify few costs associated with a lack of information security.

This investment at a level greater than O_L could indicate, among other possibilities, that the interviewed firms are explicitly adopting a more expansive view of their security boundary than that of their local good, or that they value freedom from successful attacks higher than is strictly economically justified. Based on the reactions of interviewed security managers to issues of internal and external security concerns (shown in Table 5), we posit that although security managers are mainly concerned with internal risks (a local viewpoint), they are not titrating to find the optimal investment point O_L but are investing to eliminate all successful attacks. In order for organizations to find the optimal level of spending they need to accurately know the costs incurred due to a lack of information security, their spend on information security, and have a good idea of what the marginal rate of return would be for a change in the spend. In reality, it is relatively easy to know what an organization spends on cyber security; knowing the true cost of information security lapses is a much more difficult question. There are fairly concrete costs, such as the time that is spent rebuilding systems and recovering data, and less tangible costs such as the costs of intellectual property losses or loss of future business due to brand damage. Well-known surveys such as the CSI/FBI survey include such costs, but it is acknowledged that they are more indicative of trends rather than accurate estimates of true economic costs.

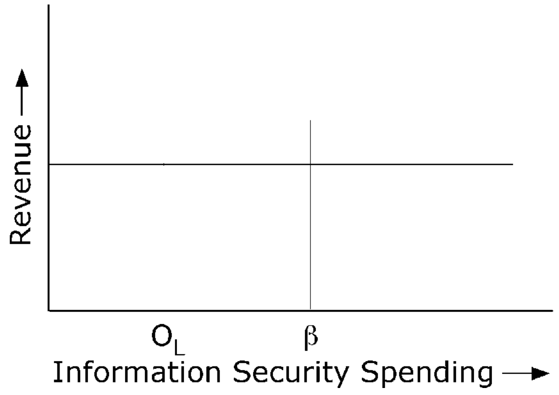


Figure 2. Increased information security has no effect on revenue. This will be the case if information security is not important in selecting suppliers. O_L and β are shown for continuity.

If there are economic incentives for investing at a level higher than that required for a local optimum, what would they look like? Any economic incentive would imply that increasing information security would result in a greater profit, either from increased revenue or reduced costs. The executives we interviewed felt that in their industry, there was little possibility to increase revenue through higher levels of security beyond a qualifying level (Q) required by some customers. Thus the firms felt that they faced either Figure 2 (no revenue impact) or Figure 3 (a qualifying level of security that enabled them to work with some customers). The Host said that some customers had required it to fill out questionnaires regarding its information security practices; the Host interpreted these questionnaires as describing a set of required practices. As part of becoming a vendor for a customer, Supplier B was subjected to a security audit to see whether its practices were acceptable. Both the Host and Supplier B indicated that they were able to qualify with their existing information security practices.

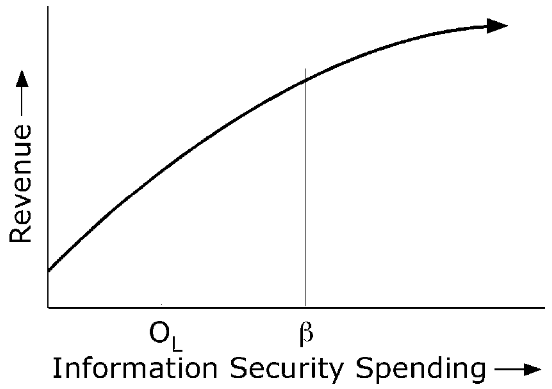


Figure 4. Increased information security yields greater revenues. This will be the case if increased information security confers a competitive advantage.

Assuming that if they did not qualify they would not have become vendors, a qualification requires that a firm must invest at a certain level in order to realize the new business associated with acquiring a new customer. This would be represented as a step function in revenue, as is shown in Figure 3. It is entirely possible that there would be a series of customers with qualifications requiring an incrementally increasing investment in security; in this case the step function in Figure 3 would start to resemble the curve in Figure 4. Here, increasing investments in security have a positive impact on revenue over the entire investment space. Only one of the executives we interviewed felt security investments in their industry led to increased revenue through such a competitive advantage.

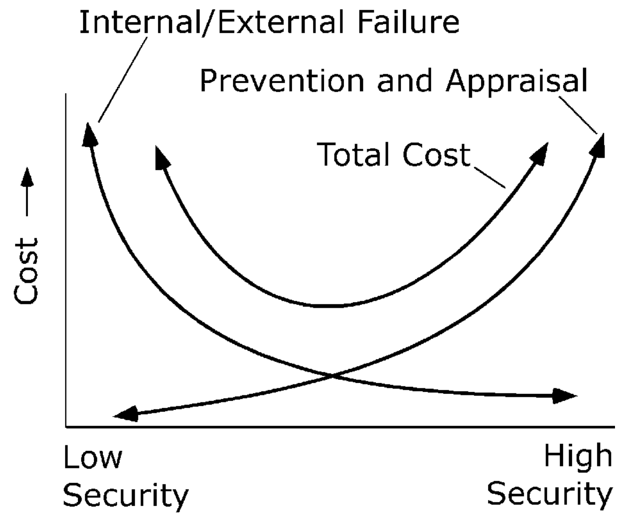


Figure 5. Information security investments in a framework from the quality literature.

Most of the executives we interviewed focused purely on the cost trade-off of security, disregarding the possibility of increased revenue. Coupling Gordon and Loeb’s model with ideas from the quality literature (Jur2000), these costs can be broken into two major groups: Costs of avoiding security failures such as on-going security appraisals and investments in preventive measures like installing a firewall. On the other hand, there are costs associated with security failures – either internal failures that are not observed by customers or external failures which are observed by those outside the firm (Table 6). Internal failures are security problems that are discovered internally, resulting in costs such as lost productivity (for example lost worker productivity and restoring information services). External failures, such as exposing confidential information can lead to many costs including litigation, fines, and brand damage. Figure 5 shows the resulting total cost; as in the work by Gordon and Loeb, there is an optimal level of investment.

One interviewee at the Host further argued that even when information security does not increase revenue there can still be a positive business value for increasing information security. This executive felt that even though increasing information security would likely not increase profits directly, the processes put in place would take costs out of the business. As an example she talked about single sign-on: while this was being done for reasons of information security, it would reduce her costs as well as increase the efficiency of her staff. Multiple participants at a recent CIO roundtable also made this point: some believed that the activity of adopting more rigorous information security will reveal opportunities for increasing efficiencies; others believed that the adoption of technologies for information security will result in better knowledge of business processes such as supply chain management, benefiting the business [Dyn04].

Are market forces present? It appears that internally, firms are more responsive to information security issues than is required to minimize tangible costs. This is likely due to the consideration of intangible costs in deciding on an appropriate level of information security. As a participant in a recent Cisco/Tuck CIO Summit said, “Failure in security, that gets noticed. If you're successful, it's expected.” [Dyn04]. This mindset will drive organizations to adopt a much stricter level of information security than that needed to minimize tangible costs. From an external point of view, it appears that there is a growing trend to require that business partners have a base level of information security.

Government Investment

Our results say nothing about the effectiveness of government investment as a means of promoting increased information security.

Liability

None of the interviewed firms felt that a lack of information security on their part would result in their being liable for damages, with the possible exception of liability resulting from Sarbanes-Oxley. None of the interviewed firms specifically held a cyberinsurance policy.

Risk to Supply Chain Continuity

The robustness of supply chains and extended enterprises is an important constituent in what would constitute a level of information infrastructure security consistent with the public good. If crucial infrastructure supply chains and extended enterprises can be incented to adopt levels of information security so they are robust against information security lapses, they would also be robust from the perspective of the greater public good with respect to information security. What do our initial results say about the risks faced by firms that utilize the information infrastructure to manage their supply chain?

One interesting result was the variability in the use of the internet by the different firms. The Host, a Fortune 500 company, utilizes the internet extensively for both its supply chain and for interacting with some large customer. Supplier A, which is also a very large company, does not use the internet at all in the management of its supply chain. Suppliers B and C utilize the internet for more than half of their supply chain ordering.

At a superficial level, executives at the interviewed organizations were very confident that they would be able to manage their supplier and customer relations in the event of an internet outage, particularly at the larger companies. All were certain that their firm would do whatever was necessary to enable their producing and shipping product. All spoke about using phone, fax and FedEx as their fall-backs if they were unable to communicate via the internet. All thought that the most pain would be experienced in the invoicing and payments process as these processes would not be a priority, and picking up all the pieces later would be tedious and error-prone.

Is it possible to substitute the three Fs (fone, fax, FedEx) for the internet?

At the smaller suppliers (C and D) it seems very possible that they would be able to use the phone and fax for their supply chain communications; Supplier D is a very small firm without a web presence, and their small volume and lack of technical sophistication makes it seem reasonable that they would be able to effectively communicate with phone and fax.

It seems likely that Supplier C, the printing and graphic design firm, would also be able to function using the three Fs. They recently experienced an outage of broadband internet connectivity for a period of weeks; while this was a major IT event, it was not a major corporate event. The actual supplies that they order are printing stock, film, inks and adhesives; orders for standard supplies are communicated by phone or email; in either case a paper copy is sent via mail. Custom supplies are obtained by talking with the vendor via phone to work out the details, and then making the order as above. Customers and Supplier C exchange designs via email or FTP; email is used to communicate with a remote design location. Supplier C said that they would revert to dial-up access to their machines or to FedEx if the internet were unavailable. As noted above, the largest impact to Supplier C would be the way they maintain their relationships with their customers.

Supplier A is interesting in that today it manages its supply chain using only fax and phone, while it does communicate with its customers, including the Host, using EDI and web-based applications (90% of its communications with the Host are via EDI or web-based applications). It would seem that an internet failure would not impact its supply chain at all, but would impact its ability to communicate with its customers. A member of Supplier A’s risk management group said that they have thought about this, and while they made sure that they have enough phone lines to adequately deal with the expected volume of calls should internet communication be disrupted, they did not do the same for fax machines or fax servers. Thus, Supplier A has identified this risk to its ability to maintain business operations in the face of an internet outage, and has taken steps to mitigate that risk.

The Host is the most dependent on the internet for management of its supply chain, and is planning to become even more dependent: executives at both of the Host’s business units aim to interface with all their suppliers using either web applications or EDI. As noted above, the Host is often a major supplier to itself; this is one reason that the Host has invested in an intranet that is separate form the internet. Another reason is the reliance on centralized applications: a supply chain manager stated that he would not know how to enter data into the Host's internal systems if their intranet was unavailable.

Would the Host be able to rely on the three F's to maintain business as usual should the internet fail, as they hopefully assert? Probably not. During one interview, a supply chain executive calculated that the number of faxes that would have to be sent to replicate the information carried via the internet would be roughly 30,000 a week from each plant; the supplier has well over a dozen plants, and due to the centralized nature of their enterprise applications, these faxes would all be sent from fax servers at one location. The issue of whether the supplier could deal with all the faxes coming from multiple customers was also raised: those suppliers with few customers are more likely to be able to manage a reversion to three F communication than suppliers with many customers.

The lack of ability to run the business as usual does not mean the business will not run. Supply chain managers at both of the Host's BUs talked about how the Host forecasts supply requirements with high-volume suppliers. As noted above, one supply chain manager was quite confident that the "learned behavior" of the supply chain would result in deliveries happening as scheduled without the need for communication.

There are certain costs associated with doing business using the three F's; these were not explored in a systematic manner. The interviews suggests that none of the interviewed firms has thought of this either; at most, interviewees talked about the overtime that would be needed to enter faxed invoices into the firm's computers for processing, and the increased error rate associated with this activity.

Logistics Suppliers

Above, we discussed the ability of the interviewed firms to use phone and fax in the case of an internet outage. What about the third 'F', FedEx, and other providers of transportation and logistics services? Providers of these services are becoming increasingly important in supply chains: one of the interviewed firms was on the verge of contracting with a third-party logistics provider (3PLP) to handle the shipping, warehousing, and delivery of a very substantial portion of its supplies. Essentially, this firm has outsourced its supply chain management to the 3PLP: the inventory of supplies at a plant will be completely managed by the 3PLP. This will require a tight integration between the firm's materials requirements planning systems and the 3PLP's systems.

Will 3PLPs and other providers such as FedEx perform in the face of a widespread internet outage? The central role that such firms play in the ability of other firms to operate makes an examination of the robustness of these providers particularly important.

The Big Picture

This study examined how firms identify and manage information security risks internally and within their supply chains. Our initial results, which we caution readers are from a sample size of 5 and are likely industry specific, lead us to believe:

- Firms are adopting levels of information security that are appropriate for their internal operations.
- Market forces, in the form of customer requirements or qualifications, are the primary driver for additional information security measures.
- The interviewed firms were reactive in their approach to information security.
- Firms need to pay more attention to the risks they are exposed to as a result of using the information infrastructure to manage their extended enterprise.

As of the date of this report, firms seem to have reacted sufficiently to existing internal threats. We think that at this point information security conversations would benefit most from turning from threats to internal systems to threats to external relationships by examining the risks in the ways they conduct business within their extended enterprise. The important question for them to ask in regards to risks is, "Who owns the risk?" [120]

In the absence of solid knowledge about the threats and probabilities of occurrence needed to make reasoned estimates of risk, firms should think about managing the outcomes of information security events through redundancies.

References

[AOL04] AOL/NCSA Online Safety Study
http://www.staysafeonline.info/news/safety_study_v04.pdf

[Bla2001] Blakley, B. (2001) "An imprecise but necessary calculation," *Secure Business Quarterly: Special Issue on Return on Security Investment*, 1(2), Q4. A publication of @stake.

[Dav2004] Davis, E.W. and R.E. Spekman, Extended Enterprise. FT Prentice Hall, NY, NY (2004).

[Dyn2004] Dynes, S. B. C. "Security and Privacy: At Odds With Speed and Collaboration?"
http://mba.tuck.dartmouth.edu/digital/Programs/CorporateRoundtables/SecurityAndPrivacy/Overview.pdf

[Fre2004] Freeman, Michael, S. Dynes and E. Goetz, "*The Known Unknowns of Cyber Security and Cyber Terrorism*" Dartmouth Institute for Security Technology Studies working paper. http://www.ists.dartmouth.edu/library/119.pdf

[120] The provenance of this pointed yet practical formulation of the issue lies with Dan Geer

[Gee2001] Geer, D. E. Jr. (2001) “Making choices to show ROI,” *Secure Business Quarterly: Special Issue on Return on Security Investment*, 1(2), Q4. A publication of @stake.

[Gor2002] Gordon, L. A. and M. P. Loeb, “The Economics of Information Security Investment,” *ACM Transactions on Information and System Security*, (November 2002), pp. 438-457.

[Gun2004] Gunther, R. (2004) “At Risk,” *Wharton Magazine*, Spring 2003.

[Joh2004] Johnson, M. E. “The safety of secrets in extended enterprises,” Financial Times, 18 August 2004, A7.

[Jur2000] Juran, J.M. and F. M. Gryna (2000), Quality Planning and Analysis, Forth Edition, McGraw-Hill, NY, NY.

[Kun2002] Kunreuther, H. (2002) “Interdependent Security: The Case of Identical Agents,” *National Bureau of Economic Research*, Insurance Project Workshop, Cambridge, Feb 1.

[Kun2004] Kunreuther, H. (2004) “Risk Analysis and Risk Management in an Uncertain World,” Forthcoming in *Risk Analysis*, Wharton School Working Paper.

[Soo2001] Soo Hoo, K. J., Sudbury, A. W., and Jaquith, A. R. (2001) “Tangible ROI through secure software engineering,” *Secure Business Quarterly: Special Issue on Return on Security Investment*, 1(2), Q4, 2001. A publication of @stake.

Appendix B Further Information on CERTs and CSIRTs

Cyber Security Incident Response – Some solutions

Various organizational forms have been developed at a multitude of organizational levels to investigate, analyze, and respond to cyber security incidents. Many of these organizational structures have developed bottom-up by professionals feeling a shared responsibility. Below, we discuss various forms of Computer Security Incident Response Teams (CSIRTs) and Information Sharing and Analysis Centers (ISACs).

1. Computer Security Incident Response Teams

As an aftermath of the so-called Morris-worm which took the Internet partially down, a number of people felt a world-wide responsibility for creating an incident response capability and standard procedures for dealing with major incidents on the Internet.· This led to the establishment of the Carnegie Mellon's CERT/CC in 1988).[121] [122] Derived from the name of this first CSIRT, the name Computer Emergency Response Team or CERT is commonly used for teams providing computer and network incident response services. However, CERT is a trademark of the Carnegie Mellon University with the intent to control the quality of CERTs by only granting approval to use the word

[121] RFC2350 defines a CSIRT as: “A Computer Security Incident Response Team (CSIRT) is a team that performs, co-ordinates, and supports the response to security incidents that involve sites within a defined constituency”. The CERT Coordination Center (CERT/CC) ([3]) defines a CSIRT as: “a service organization that is responsible for receiving, reviewing, and responding to computer security incident reports and activity”.

[122] Background information about CERT-CC can be found at www.cert.org along with best practice information about how to organize and manage CSIRT organizations (http://www.cert.org/csirts/). Considerable useful information is available on the website of the Australian CERT, (http://www.auscert.org.au/) along with an inventory of background documents and presentations (http://www.auscert.org.au/render.html?cid=1938)

CERT after an accreditation process.[123] The term CSIRT is generally used herein to address all computer security incident response team names, although the term CERT will be used as well.

CSIRTs can have a very limited set of tasks and limited constituency. More often, they are part of a network of trust where CSIRT-partners share a mutually trusted relationship, a so-called "web-of-trust".[124.]

CSIRT coordination mechanisms worldwide

Initially, the CERT-CC had the leading role in coordinating research as well as responses to computer-related incidents. Currently, that task is more distributed as other CERTs, software and hardware manufacturers, and research organizations have taken up some of that work. There is an abundance of information available about the role and functions of CERT-CC which provides technical assistance to other CERTs around the world.

A directory of CERT operations is overseen by an umbrella organization known as FIRST. [125] It has been an important priority of the U.S. government to develop the capabilities and know-how of CERTs around the world. However, the number of CERTs has been growing so quickly in recent years that it is not possible anymore for CERT/CC and FIRST to co-ordinate all CERT activities on the globe. Therefore, regional co-ordination centers including TERENA, a coordinating body for CERTs in Europe, and AUS-CERT as focal point for Asia-Pacific Computer Emergency Response Task Force (APCERTF), etc. come into play. Through various regional organizations such as the Organization of American States (OAS) and the Asia Pacific Economic Cooperation Council (APECC) significant initiatives have been being taken to establish and/or identify CERT organizations operating at the national level. Such CERTs may have the government as their constituency or may have a broader constituency including private entities while being supported by governments. They help to develop local CERT capabilities through domestic and regional level training activities. On a regional basis, there are efforts to share "good practices" among CERTs as well as develop common procedures for sharing information and responding to incidents as they develop. In Europe, these tasks have been taken up and are assigned to the Trans-European Research and Education Network Association (TERENA).

[123] Some examples of other common used names besides CERT and CSIRT are CIRC (Computer Incident Response Capability); CIRT (Computer Incident Response Team); IRC (Incident Response Center); SERT (Security Emergency Response Team); and SIRT (Security Incident Response Team).

[124] Handbook for computer security incident response teams (CSIRTs); Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski; December 1998; http://www.cmu/SEI-98-HB-001; wuarchive.wustl.edu/languages/ada/sei/documents/98.reports/pdf/98hb001.pdf.

[125] The web site of international CERT organizations can be found at www.first.org . In addition, considerable information about CERT organizations in Europe is available at http://www.terena.nl/tech/task-forces/tf-csirt/

Although the newly created European Network and Information Security Agency (ENISA) is not intended to operate as a regional or super-CERT, it is likely to focus considerable resources on sharing of information and expertise among the web of main CERT organizations operating within the now expanded scope of the European Union and fostering fast reaction capabilities.[126]

In Europe, there is also a regional co-ordination center to support the European CSIRTs. These tasks have been taken by the Trans-European Research and Education Network Association (TERENA). Although originating in the academic research and development community, TERENA's activities extend to other constituency communities as well. TERENA coordinates large international innovation-related projects concerning telematics and infrastructure. TERENA, which is located in Amsterdam, is monitored by the European Commission (EC). Regional co-ordination centers usually have the following tasks: (1) coordination and support to regional CERTs, (2) accreditation of CSIRTs, (3) support tool development. The accreditation activities of TERENA are called the Trusted Introducer (TI)[127] and are largely based on a screening process of information supplied by a prospective CERT.

Whatever the strategic importance of CSIRT mechanisms, there are critical questions that need to be addressed concerning CSIRTs and firms in critical infrastructure sectors as well as with other public sector entities dealing with cyber security. In many developed countries there is not a single CSIRT. There are, in fact, a range of CSIRT mechanisms of differing sizes and with differing constituencies.[128]

CSIRTs may choose to do one or more of the following three basic tasks:

1. Co-ordination of CSIRT activities (co-ordination of the organization, incident responses or both).
2. Technical operations (resolving threat and incident responses).
3. Quality assurance & management.

[126] For further information about the newly created European Network Information Security Agency see http://www.enisa.eu.int/ . The future role of ENISA was addressed at an October 2004 conference organized by the Dutch government concerning e-security, http://www.esecurity-eu2004.nl/ . Considerable relevant background information was included as background information at the conference.

[127] http://www.ti.terena.nl/

[128] The next is based upon information collected by Martis, E.R., Luiijf, H.A.M., and Geers, J.M.E., TNO, The Hague, The Netherlands in 2004 for an investigative project on Computer Security Incident Response Teams.

The related task of certifying a CSIRT has to be undertaken by a certification body. That body can not be a CSIRT itself. Below some existing types of CSIRT that exist are listed.

Following are some examples of different types of CSIRTs:

- Internal CSIRT: an internal CSIRT provides services to its parent organization. The constituency of an internal CSIRT is a corporation, government, education organization, etc. This type of CSIRT performs its services for the organization ’in-house’.
- Branch or sector CSIRT: a branch CSIRT provides services to parties working in the same type of business, e.g. all banks in a country.
- National/Regional CSIRT: a national or regional CSIRT provides incident handling services to a country or region. It will mainly have a trend-analysis, informational and some high-level coordinating role.
- International CSIRT: an international CSIRT provides services to CSIRTs from different countries. It will mainly have a coordinating role.
- Co-ordination Centre: a co-ordination centre has an informational role; it co-ordinates and facilitates the handling of incidents across various CSIRTs. An example of a Co-ordination Centre is the CERT/CC in the United States.
- Analysis Centre: an analysis centre focuses on synthesizing data from various sources to determine trends and patterns in incident activity. This information can be used to help to predict future activity or to provide early warning when the activity matches a set of previously determined characteristics.
- Information sharing (and analysis) centre: an information-sharing centre offers sanitized and anonymous information on threats and incidents. Often these information-sharing centers operate sector-wise and combine this service with

some analysis capability in a so-called Information Sharing and Analysis Centre (ISAC). (See the further discussion below).

- Product / Technical CSIRT: a product CSIRT provides incident handling services for parties using the same set of products. This can e.g. be parties using Linux as operating system.
- Vendor Team: a vendor team handles reports of vulnerabilities in its software or hardware products. It also provides solutions to weakness in it's own products.
- Service providers: a service provider provides incident handling services to all parties using a certain service like a network or the Internet. This can e.g. be a research network or the network of the service provider.
- Commercial / Contractual CSIRT: a commercial CSIRT provides incident handling services to paying clients on a commercial basis. Most of the time such a CSIRT will have a certain specialization, e.g., companies in a certain branch or companies using the same set of products.
- Incident Response Provider: an incident response provider offers incident handling services as a for-fee service to other organizations. This can be e.g. business continuity services in case the ICT infrastructure of a company has become unavailable through an incident.
- Warning centre: a warning centre has an informational role for specific malware, e.g. virus warnings.

Some of these CSIRTs overlap, i.e. a CSIRT can for instance both be a commercial CSIRT and a product-related CSIRT. CSIRTs also provide many different services to their constituents—some reactive[129] and others pro-active.[130]

[129] Reactive services include: (1) incident classification and triage, (2) incident co-ordination, (3) incident response, (4) incident recovery, (5) incident tracing

Most CSIRTs will be formalized teams. However, for some CSIRTs, like the internal CSIRTs, also an ad-hoc team can be formed in case of an incident. Besides these types of CSIRTs, a CSIRT can also choose to provide another category of service(s) to its constituency such as a governmental CSIRT. These characteristics define the constituency of a CSIRT and the relationship between the CSIRT and its constituency.

CSIRTs have to interact with other CSIRTs. The amount of interaction depends on the characteristics of the CSIRT. Apart from communicating with its own constituency community, the CSIRT could communicate with:

- Other CSIRTs including industry/government sector CSIRT (asking advise, exchanging experiences, co-operative work);
- The national CSIRT if existing.

[130] Some pro-active services include: (1) enhancing security awareness, (2) incident trend analysis, (3) pre-alarm and warnings based upon vulnerability reports and incident reports, (4)patch provision, (5) security consulting, (5) security products, improvements in procedures, plans, and quality, (6) security vulnerability and incident warnings, (7) intrusion detection, (8) vulnerability screening, (9) security audit, (10) penetration testing, (11) business continuity planning, (12) configuring and maintenance of security tools

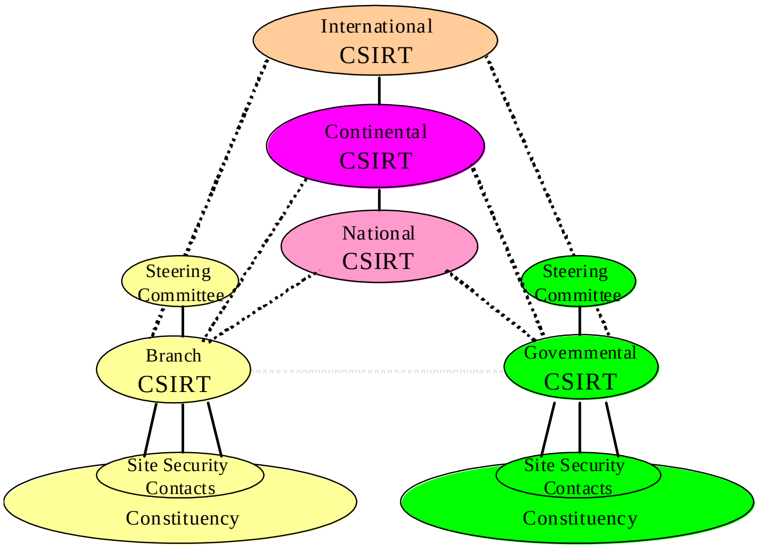


Figure Appendix B-1: Inter-CSIRT interactions

2. Information Sharing and Analysis Centers

Information Sharing and Analysis Centers are a special kind of CSIRTs in which a specific sector, e.g., the financial sector or the energy sector, creates an independent commonly-funded entity which acts as a clearing house for information-sharing between the connected partners. The ISAC offers sanitized and anonymous information on threats, sector-specific vulnerabilities, and incidents. Often the ISACs combine this service with threat, incident, and trend analysis capability. ISACs may share and exchange information with government agencies, but do not necessarily need to do that.

Some ISAC-like organizations exist already for quit some years in various countries, reason for the United States administration to push all critical sectors to establish such ISACs top-down. Reports show that some of these newer Information Sharing and Analysis Centers do not always function smoothly and efficiently as mechanisms for information flow and are viewed as ineffective and bureaucratic, partially due to the problem managing and maintaining trust. [131] Informal organizations such as BITS[132] [add further background information] operate through high-level informal ties at a senior executive level in the financial services sector. Various advisory firms as well as software and hardware suppliers can also act as an effective conduit for information among firms in the same or related industry sectors. As is emphasized in World Bank studies of cyber security arrangements in the financial sector, effective intra-corporate arrangements and procedures for responding to cyber incidents are one of the key elements of a well designed set of ICT corporate governance arrangements. [add reference to World Bank study] Thus, any initiatives to develop new or enhance existing CSIRT-organizations and capabilities at sector-level will need to focus special attention on the integration of CSIRTs into incident-related flows of information within firms, from individual firms to related firms in the same sector, and these firms to firms in other sectors.

At the enterprise level, there are a number of different ways of structuring the CSIRT-related functions depending on the size and scope of the enterprise.[133] For example, the cyber risk management functions can be handled on a centralized basis, be embedded in various corporate subsidiaries, or overseen through a hybrid structure with central staff and decentralized cyber security units. In many corporate setting, especially in small and medium sized enterprises (SMEs), some or all cyber security responsibilities may be outsourced to private service providers or external CSIRT organizations.[134]

[131] See background information relating to industry sector ISACs in footnote above.

[132] For background information about BITS http://www.bitsinfo.org/ and its initiatives in the security area (http://www.bitsinfo.org/secrelini.html)

[133] Work by Martis, E.R., Luiijf, H.A.M., and Geers, J.M.E., TNO, The Hague, The Netherlands in 2004 on Computer Security Incident Response Teams and Tuck Research Study

[134] For example, in the United States, the CERT-Coordinating Center has a close collaboration relationship with the U.S. CERT which oversees and coordinates responses to computer incidents from an institutional base within the Department of Homeland Security.

In addition, the relationships among CSIRT mechanisms—whether within a sector or external to a sector—can be viewed as structured on a hierarchical or a peer-to-peer basis though in practice information relating to incidents is likely to flow over both avenues. Inevitably, information will not just flow only through a common coordinating point. It will also move more informally among firms, especially based on personal or professional contacts unless there are either corporate or regulatory restraints on such flows. Especially in countries where a national CSIRT organization is being initially established, it may be very important for policy-makers to recognize that a national CSIRT is only a first step in a dynamic process. This coordinating mechanism will need to build its own trust relationships with firm-specific CSIRTs or other bodies already dealing with cyber security-related concerns.

Likewise, it is likely to be important that collaboration among CSIRTs at the national level may not be hierarchical. There are likely to be significant peer-to-peer flows of information, especially within multi-national firms, but also within specific CSIRT bodies that might deal with cyber-related incidents on a cross-border basis. For example, in Europe a number of financial institutions in different EU-member states are beginning to share information relating to fraudulent cyber-related banking transactions.

GLOSSARY

3G/4G	Third/fourth generation of GSM
APCERTF	Asia-Pacific Computer Emergency Response Task Force
APEC	Asia-Pacific Economic Cooperation
APECC	Asia Pacific Economic Cooperation Council
CCIPS	Computer Crime and Intellectual Property Section
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CERT CC	CERT Coordination Centre
CFO	Chief Financial Officer
CI	Critical Information
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CITEL	Commission Interamericana de Telecomunicaciones
CNIL	(FR) La Commission nationale de l'informatique et des libertés
COSO	(U.S.) Committee of Sponsoring Organizations
CSIRT	Computer Security Incident Response Team
DHS	(U.S.) Department of Homeland Security
EC	European Commission
EDT	Electronic Disturbance Theater
ENISA	European Network and Information Security Agency
EU	European Union
FCC	(U.S.) Federal Communications Commission
FOIA	(U.S.) Freedom of Information Act
G8	Group of Eight (U.S., Japan, Germany, France, U.K., Italy, Canada, Russia)
GAO	(U.S.) Government Accountability Office
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
I3P	The Institute for Information Infrastructure Protection

ICT	Information and Communications Technologies
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISAC	Information Sharing and Analysis Center
ISACA	(U.S.) Information Systems Audit and Control Association
ISP	Internet Service Provider
ISPAN	Internet Service Providers' Association of Nigeria
ISSB	(PRC) Information Security Supervision Bureau
ISTS	Institute for Security Technology Studies
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
NACOTEL	(NL) Nationaal Continuïteitsplan Telecommunicatie/ National Telecommunications Contingency Plan
NASSCOM	(India) National Association of Software and Service Companies
NATO	North-Atlantic Treaty Organisation
NCWG	Nigerian Cybercrime Working Group
NGN	Next Generation Networks
NHTCC	(UK) National High-Tech Crime Center
NIAC	(U.S.) National Infrastructure Advisory Committee
NIDTA	(Nigerian) National Information Technology Development Agency
NISCC	(UK) National Infrastructure Security Co-ordination Centre
NRIC	(U.S.) National Reliability and Inter-operability Council
NSTAC	(U.S.) National Security Telecommunications Advisory Committee
OAS	Organization of American States
OCTAVE	Operationally Critical Threat Asset Vulnerability Evaluation
OECD	Organization for Economic Cooperation and Development
OPTA	(NL) Onafhankelijke Post en Telecommunicatie Autoriteit
PRC	People's Republic of China
QoS	Quality-of-Service
R&D	Research and Development
RANS	Russian Association for Networks and Services
ROI	Return-on-Investment
SCADA	Supervisory Control And Data Acquisition

SME	Small or Medium sized Enterprise
SMS	Short Message Service (GSM)
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TERENA	Trans-European Research and Education Network Association
UCTE	Union for the Coordination of Transmission of Electricity
UTC	Universal Time Coordinated
VOIP	Voice-over-IP
VPN	Virtual Private Network
WARP	Warning, Advice, and Reporting Point
WSIS	World Summit on the Information Society
Y2K	Year 2000

REFERENCES

Reference material used in the preparation of this discussion paper is included in a wiki site that can be accessed on-line at www.dartmouth.edu/tiki. This material has been organized into a series of categories that correspond generally with some of the major sections of this discussion paper. The authors intend that this wiki site might continue to be developed through an international consortium of research institutions as has been recommended in Part V.C of this paper. The authors believe that this discussion paper should be viewed as a working paper that will encourage an on-going and collaborative process of collection of important documentation relating to cyber security issues. It is hoped that the collaborative nature of the wiki site will permit the initiation of a widespread effort of research institutions and other entities concerned with cyber security issues to contribute to a shared data base of information relating to an increasingly wide circles of countries.