Security through Information Risk Management

Forthcoming in *IEEE Security and Privacy*

M. Eric Johnson
Center for Digital Strategies, Tuck School of Business at Dartmouth College

Eric Goetz
Institute for Information Infrastructure Protection, Dartmouth College

Shari Lawrence Pfleeger
RAND Corporation

Keywords: Information Risk, Security, CISO, Organizational

Abstract

While security professionals have long talked about risk, moving an organization from a "security" mindset to one that thoughtfully considers information risk is a challenge. Managing information risk means building risk analysis into every business decision. Here, the authors explore how chief information security officers (CISOs) of large firms are working to move the conversation from security towards information risk. While CISOs face many organizational challenges, we find wide agreement that action plans must include risk categorization, communication, and measurement.

Introduction

As information security risks evolve from curious hackers testing their prowess to malicious organizations seeking financial gain, many organizations' security programs are focused less on fortress-building and more on managing risk. But evaluating risks requires understanding attackers. And because some attacks, such as intellectual property theft, may not be discovered until well after they happen, protecting against economically-driven threats requires much more than technology; it requires building a security culture in which everyone can recognize and evaluate the risks[1].

Through a series of field studies, executive interviews, and a security working group we have been studying how security executives in large firms are shifting their approach to help their organizations make better risk decisions. This article presents our working-group (Table 1) findings and includes many direct quotes from security executives who attended a related workshop (The workshop involved dozens of CISOs from Fortune 500 companies along with researchers and government policy makers. Unless otherwise noted, executives quoted held a top information security role within their firm). The roll-up-your-sleeves event touched on issues such as ranking and prioritizing risks, communicating within the organization, and measuring security progress. We focused on the link between information risk and business risk, rather than on management approaches to deal with threats to critical infrastructures or the risks facing

The workshop and research described in this article were partially supported under Award number 2003-TK-TX-0003 from the U.S. Department of Homeland Security, Science and Technology Directorate. Points of view in this document are those of the author(s) and do not necessarily represent the official position of the U.S. Department of Homeland Security or the Science and Technology Directorate.

governments and the general public. The results were two-fold: identifying best practices and sharing innovative ideas that could make security a mainstream corporate risk management practice.

Table 1: Working Group Members[2]

Adidas Group
BJ’s Wholesale Club
IBM Corporation
3M Information Technology
Aetna, Inc.
Bose Corporation
Staples Inc.
Colgate-Palmolive
Cargill
Department of Homeland Security
The Dow Chemical Company
Eaton Corporation
BT Group
Eli Lilly and Company
I3P
RAND Corporation
CVS Caremark
Bechtel Group, Inc.
CXO Media Inc
H&R Block
General Dynamics
University of Virginia
Defense Information Systems Agency
Cisco Systems, Inc.
Goldman Sachs
United Technologies
Time Warner Cable Corporate

The Evolving Risk Landscape – Risks and Confounding Factors

Information security risks within large corporate firms have shifted significantly as adversaries have become more sophisticated. Across the firms we worked with, executives identified several pressing challenges they hoped to address in 2008. The most pervasive challenges included:

Protecting intellectual property, particularly when outsourcing. In a knowledge economy, IP is increasingly the lifeblood of any company. Protecting IP requires the effective use of technology, but user awareness and education are critical, too. Employees must understand not only what IP is but also its value to the company that owns it. As Bechtel’s CIO Geir Ramleth explained, “It’s awareness, building awareness among your employees of what does IP mean. Who owns IP, how do we treat it, and who should see it and who should not see it?" It is also difficult to protect IP in emerging markets or while doing joint ventures with possible competitors. Robert Nowill from BT noted that, "the things that keep me awake at night have to do with offshoring and outsourcing" because other countries have different cultural attitudes towards IP, exacerbated by different, weak, or inadequately enforceable IP protection laws. And the expanding size and complexity of supply chains can create more potential points of risk for corporate IP.

Data leakage. Data breaches can negatively affect a company's reputation and brand. Leakage[3] can occur at any level—network, desktop, handheld device—and any method—e-mail, back-ups, or lost memory stick[4]. Time Warner Cable's Nancy Wilson fears the problem's scale: "We have about 10,000 laptops we're encrypting now, or trying to encrypt. And [without encryption, the risk of] data leakage is huge."

Compliance. Firms in many sectors from health care to financial services face growing compliance complexity. For example, retailers have been scrambling to comply with payment card industry (PCI) standards. The patchwork of state breach reporting legislation creates cost and confounds compliance for many firms[5]. Others are constrained by regulations such as the SarbanesOxley Act or the Health Insurance Portability and Accountability Act (HIPAA). Compliance challenges are not just financial; Bose's Terri Curran noted, "we make products that now are being required contractually to have digital keys. Every automotive amplifier that we put out has to have a digital key on it now because of regulations for Blu-ray and other technologies. So I have compliance all the way down to the manufacturing floor."

Visibility for security. At some consumer products or manufacturing firms, security may not always receive adequate attention and support from senior management. According to Rodney Baker from Adidas: "It's just sneakers and T-shirts that we make, so trying to get people's attention inside the company is part of the biggest challenge." Moreover, as companies expand and diversify operations and locations, it is a challenge to maintain security across the business. Says Staples' Chris Dunning, "We're in 22 countries right now, so the risk that I'm trying to manage is understanding where is that weakest link, trying to move what we've done here in the U.S. into those various countries, and then getting the CIO and the CEO at the same level of understanding what those risks are and what they need to invest in from a global point of view."

Security at the speed of business. Every company must be agile, rapidly pursuing business opportunities, such as new markets, partnerships, third party relationships, or mergers and acquisitions. Security must move at the same speed. IBM's Linda Betz explained, "The business units expect you not to be the inhibitor of those relationships, and I don't think that I can respond to change fast enough." Aetna's Debra Cody reinforced this: "Our greatest challenge is our merger and acquisition activity, and the challenges of our sharing the proper due diligence at the earliest possible juncture around the security of those environments." H&R Block's Jeff Sherwood described different time pressures: securing distributed, fast-paced operations that function effectively for a short time: "Our business model has us ramping up to nearly 13,000 points of presence with 100,000 users every year, then tearing it all back down. Basically, we make $3 billion in 45 days and everything is about that. From the risk perspective, our environment is extremely distributed … extremely high-paced for a very short period of time. It's nothing that we sustain throughout a year. It's a big, huge light switch: on and off."

Protecting customers from themselves. Firms sometimes encounter opposition from customers or partners that don't yet see the importance of security. Nonetheless, when something goes wrong, firms bear much of the blame. Finding ways to help customers do the things that are in their own best interest is an ongoing challenge.

Yet, with the evolving risk landscape, executives with whom we have worked agree that the biggest challenge is changing the way organizations think about information risk.

Changing the Risk Mindset

While there is wide agreement that risk thinking must change, a poll of 25 security executives at a recent workshop suggested that many firms still have a long way to go. Each CISO was asked to rate her organization on a scale of 1-10. At one extreme, '1' is interpreted to mean that the CISO should simply make the organization secure and let everyone know when it is done. At the other extreme, '10' means that everyone is involved in information risk decisions, making economic and risk trade-offs; information risk is part of every business discussion. Figure 1 shows that half of the executives rated their firms 5 or lower, and no firm is rated higher than 8.

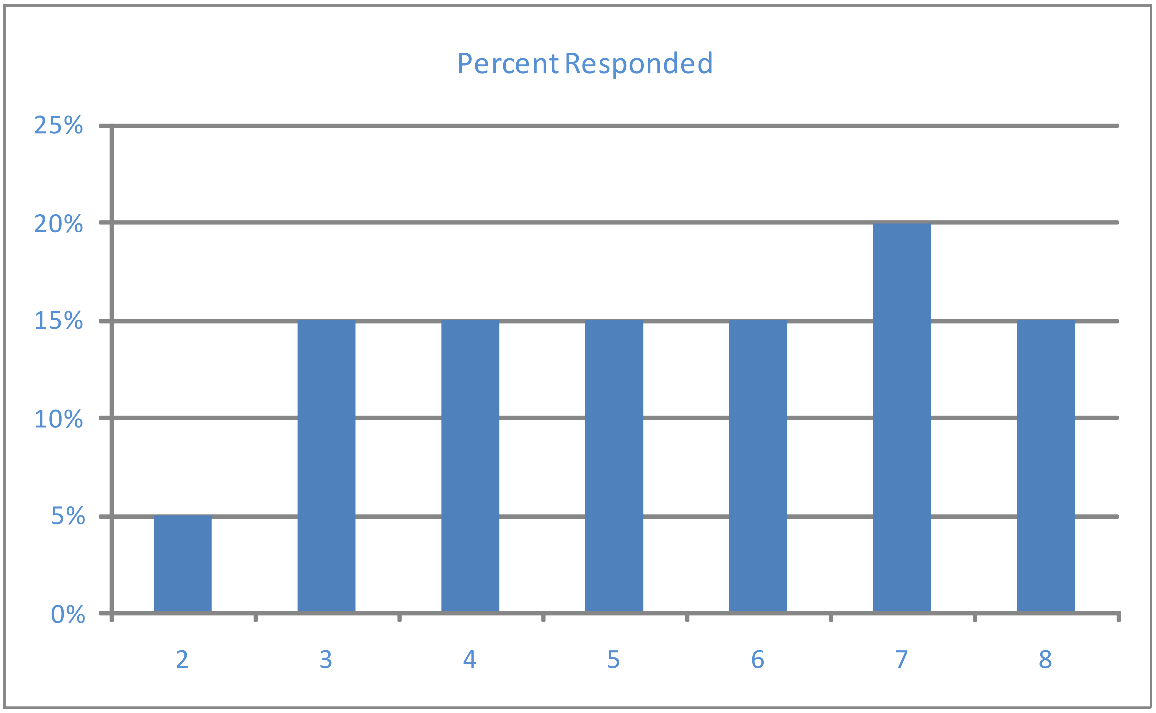

Figure 1: Ranking of information risk awareness and participation within firms.

So how can organizations improve their understanding of information risk and incorporate that insight into their broader business risk management activities? Through our research, we identified ten key points that CISOs should address.

Create market incentives for improving security. Right now, there are few significant market-based pressures to improve cyber security[6]. As a result, security executives fight internal battles to make a business case for security. Security is viewed as a cost, not as a business differentiator. Could traditional entities that price risk, such as credit rating agencies, insurance companies[7], banks and risk appraisers, create measurable economic incentives by developing a transparent, accurate, and consistent way to incorporate cyber security risks? That is, could cyber risk be part of an overall risk calculation, and priced accordingly?

DHS Assistant Secretary for Cyber Security and Telecommunications Greg Garcia noted that some cyber risk-based pricing is already happening in the credit rating and insurance fields. Risk exposure is minimized when information is accurate, but unfortunately, much of the available data is suspect.[8] Accurate risk assessment reduces exposure to unexpected losses, and helps price risk more effectively. It also provides clear standards and transparency; companies with a strong security posture can get credit and insurance at better conditions, and a higher valuation in the marketplace, providing real financial returns on their security investments[9]. Competitors who spend less on security will end up paying in other ways.

Goldman Sachs' Phil Venables described how several financial firms are working with Moody's, one of the leading credit rating agencies, to rate information risk. Firms could use ratings to choose a service company, including how much they are willing to pay for a service according to the risks posed by that provider. Venables said, "We intend on primarily using this to rate outsourced service companies. We want to have Moody's go and rate them. And from that we'll be able to adjust the amount of money we're going to pay for a contract in relation to the cost of extra mitigants. When their cyber security risk has been evaluated and rated, we can decide based on clear, consistent evidence whether we need to take on more or less of the risk for that provider and can make contracting decisions accordingly. This in turn can be augmented by similar industry efforts like BITS/FISAP[10]."

Use risk terminology. IT security jargon can lead business executives to misunderstand a problem's severity or potential risk. Said Venables, Goldman Sachs "started adopting phrases that are natural to our business people like, 'the spread of risk,' 'the 99th-percentile scenario' and 'the economical capital of risk'. Using the language of the broader spectrum of risks innate to a particular company, again, aligns up that risk to be managed alongside all the other significant corporate risks."

Similarly, senior managers are familiar with risks that are not cyber in nature. Bechtel's Ramleth said, "What you have to do is to find those analogies of how you talk about your portfolio risk, which is all the threats and stuff that we're dealing with, against their portfolio, which is the project portfolio. They have more risk than they want to deal with. So you have to get into that vocabulary. Come with an acronym, they just throw you out." Moreover, demonstrating that security is an enabler is an internal marketing effort, whereby security leaders show that difficult or risky projects worked only because security was built in, not bolted on.

Balance all risks. Information security professionals are sometimes accused of failing to keep information risk in context. Security competes with other risks for attention and resources. Finding a balance among all risks—and staying profitable—is difficult. Ramleth explained that Bechtel often runs massive projects: “We run, at any given time, about 75 to 100 large projects around the world. That’s all we do. But they are very big and very, very complex, and sometimes in very, very difficult situations and locations. ... We were in Baghdad to try to help restore various things there almost as early as the forces that came in after the battles. We also run a project up on the northwest side of India, about 30 miles from the Pakistani border, where we have 100,000 craft laborers in a community with only 100,000 people. And we have to feed them and their families every day without an existing supply chain in place. You have to balance what you do from a work execution standpoint against your security needs; it’s tough and it’s always changing.” Security leaders should generate information about threats, risks and potential consequences, enabling senior executives to decide how to balance cyber security risks against other risks.

Sometimes, a company would rather accept the risk than take a security action. However, risk tolerance should inform that choice, based on solid information rather than intuition. John Stewart explained that Cisco has a high risk tolerance: “My executive team, all the way to the top, is willing to listen to information risk management. … We acquired a services collaboration company called WebEx, which has about 4,000 people in the United States and in China. That is a high-risk maneuver when you make the acquisition happen in six days flat from beginning to end. That’s how fast you can take risks. On the other hand, we also have added 20 countries in the last two years. …[S]hareholders expect a return on their investment. It is risk and return. If you can’t articulate squarely that you’re in a high-risk environment, you can’t do risk management.”

Make security a data-driven discussion. Regularly feeding the organization appropriate data is a powerful way to drive change. For example, at Cisco, every Friday morning, executives get a voicemail briefing on the last seven days around information security events of any type. Said Stewart, “One thing you’ll know about Cisco is we’re insanely competitive, including inside the company. And as a result of hearing callouts of a senior vice president’s organization having an information security problem, they get really upset to hear their name. And they actually reflect it back into their organization, not at us.” Rankings can identify security underachievers, thus motivating employees and executives to become more proactive. As Baker of Adidas noted, “It is human nature that people want to stay off those negative lists or avoid the phone calls from security. So how do you get them from just reacting, being very reactionary, to being more of a pro-activist? How can we make security thinking become engrained in someone’s way of life? How do we get them to just think that way? It’s education.”

Of course, data-driven discussions require agreement on what to measure. Metrics has long been a challenge in information security.[11] We find that firms use numerous security metrics: the number of attacks a company is facing, the number of hits on its firewall, the number of privacy breaches, the percentage of documents or messages encrypted, or the number of people receiving security training, for instance. But some are beginning to argue that security measurement has become part of the problem. Bobbie Stempfley from DISA thinks that many measurements limit personal initiative: “Measurement becomes an abdication of personal responsibility. Everybody does exactly what is on the report card, and absolutely nothing else. They want somebody in the chain to tell them what it is they need to do in order to change a color on that report card, and that’s it.” Others worried that security metrics may be useful against the current generation of threats but cannot address new challenges. As IBM’s Linda Betz put it, “I feel good about all the stuff we’re measuring, but I worry about what we’re not measuring. How are the threats changing and how do we measure the emerging threats?”

Develop risk-based priorities. Making security part of overall risk management is a pervasive goal among security executives. Increasingly, security issues are being discussed with other risk factors, but they don’t always receive equal emphasis from senior management. BT’s Nowill explained that, “Management theory says, ‘Drive your order agenda from risk.’ People tend not to because there are other things on their mind. And even if you do, the information risk doesn’t feel quite as important as the stock price today or the politics or whatever happens to be going on in the corridor. But getting that mindset for awareness from the top down is really important. Information-type risks percolate to a certain level in the organization, but they never quite make it all the way to the top table. There always seem to be bigger fish to fry.”

As security moves more into mainstream risk management, the conversation must move from “black magic” toward business control, an approach that has been successful at Goldman Sachs. Said Venables, “We have various committees that are involved during new product development, acquisitions or other events that now routinely consider questions of information risk and control.” Some firms are further along this process because their industries are heavily regulated and security is thereby a senior management concern.

Some companies have the right “tone at the top,” while others are still struggling to communicate the real cyber risks to senior leadership. Most senior executives now understand that security is part of the discussion, as long as products and services are delivered as fast as possible (or as fast as their competitors). Agility still trumps security, so the case for better security is hard to articulate. Indeed, attitudes toward security are usually framed in terms of how a firm sees itself in its marketplace.[12] “The direction we are taking is to avoid death by a thousand scratches,” said Russ Pierce from CVS Caremark, “i.e., implementing threat-based security and control precautions one regulatory/third party requirement at a time. To this end, we embrace industry standard frameworks and best practices for evaluating and securing the organization.” For some companies, appreciation for security comes only on the heels of a damaging incident. As IBM’s Betz put it, “Some of our business unit executives actually have some religion because they’ve seen pain. When you have a bad incident, the board of directors and the senior executives get pretty upset and look to us for leadership in terms of, ‘What’s the next threat?’”

In the past, senior executives expected the CISO to ensure safety against viruses and hackers. However, now many realize that perfect security is unattainable, so the goal is risk mitigation, not risk elimination. Within the framework of risk management, the trade-offs between risk and return are already familiar[13]. Sherwood from H&R Block elaborated: “I had somebody ask me, ‘Can you protect this piece of information?’ I said, ‘Yes, as long as you promise never to use it.’ So there’s that balance that you have to have.”

Align security with company culture. Bill Gabby explained that at private firms like Cargill, culture impacts risk management. Trust and a handshake are the basis of the company, so when he suggested introducing IP leakage monitoring people were upset. They felt that such a measure would imply that the company didn't trust its employees, and would undermine company morale. About half the workshop participants said they were using some kind of content monitoring tool to help protect their information against leaks. Because of the huge volume of data that traverses most networks, companies must be quite selective about what they monitor. Often this decision is made based on data classification or on regulatory or privacy requirements. In the words of Pierce of CVS, "Given the volume of information flowing in and out of an organization and the sensitivity of the tools (i.e., false positives) you could easily get overwhelmed if you are not careful. To be successful, it is imperative that you pick your battles based on information classification/type. It is also important to gain the support of those in the organization who will share in managing the end-results of this process/technology: management, human resources, loss prevention, and legal to name a few." A key problem with monitoring tools is false positives, or what Sherwood called the "friendly fire of information security." Each needs investigation and follow-up. Several firms have implemented an automated response to data leakage that is identified by their monitoring tools. This response can be a warning message to the employee that is suspected of leaking the information, or the message can simply be blocked.

A first step for many organizations is to classify data to ensure that what is being protected is also what is most important. Data classification should be followed by a clear policy for data protection, with clear rules on who is to protect what. Moreover, the policy must be crafted so that everyone feels personal accountability for protecting data, and it must be enforced to be effective. Wilson explained how this was done at Time Warner Cable: "I found the first thing is just defining what's important to the business and doing the classification and establishing a policy. Pretty much that sets the next steps. It took us a couple of years to really nail that down. It's also ever changing in terms of different groups defining data points and levels of classification for different types of data."

One attendee of our recent workshop emphasized that data classification and subsequent protection policies are not awareness tools. Rather, they hold employees accountable. As another participant noted, "for me, it was to draw a line in the sand and actually clearly define what it was so that we could then communicate it clearly in business terms. We also block our data and we have established that if data is not labeled, then it is confidential by default." Susan Bates described BJ's approach to data protection: "We have very clear policies that prohibit the taking of data from the network, storage of data on laptops, e-mailing of data unless it's authorized and encrypted. We have clear policies. We let them know that they're being monitored, 'You can and will be monitored.' The company's assets are for company use. Everybody acknowledges at some point some little bit of personal use, but they need to know that they will be accountable if they break those rules. And you need to follow through on that. The worst thing is when people do break the rules and then they don't get fired. So it has to have teeth."

Firms that are heavily regulated have an advantage, because the security driver is clearly important to senior management. Lee Warren from United Technologies suggested: "If your culture isn't ready for it, it's not going to take. Everything goes back to the realization that data is vulnerable. And so you have to ask yourself, ‘Okay, if data is vulnerable, what do I want to protect?’ IP is the lifeblood of the company. So, what is really important to you because you can’t protect everything? It’s just unrealistic.” Jack Matejka from Eaton suggested piggy-backing on other corporate functions: “Inculcate security into the other business functions; whether it’s the ethics program and you blend into the overall ethics program training; or whether we incorporate security into SOX compliance, or some other program or function. Now we’re targeting our engineers with those controls that are integrated into other business functions.”

Highlight long-terms risk to intellectual property. Eaton’s Matejka emphasized that “intellectual property in the form of our new product designs, that’s our future, so we need to give it extra protection. We’re already seeing knockoff gears and shafts that can replace broken parts of transmissions that we might build. Anything can be reverse engineered, but why give them the advantage of getting the drawings without going through the reverse engineering?” Cargill’s Gabby humorously put IP risks into perspective: “I learned a statistic a couple of weeks ago: 45% of people leaving a company will leave with IP from that company; 65% if you include the IT professionals; and the joke was that it’s 100% if you include the marketing people.” Changing employment patterns can play an important role. As Dow’s Mauricio Guerra pointed out, “a key factor concerning intellectual property involves the whole concept of loyalty. People used to spend 35 years working for Dow. They worked in the company until they retired. Those days are gone. Companies have been very aggressive on downsizing and people now move from job to job, company to company. This dynamic changes an employee’s loyalty to his company and can elevate the risk to intellectual property.” Security programs must take into account this change.

Because IP is so much easier to steal in the digital age[14], and so many products can be rapidly reverse engineered, new approaches may be necessary. As 3M’s John Brenberg put it, “What it really came down to for us is, ‘What really makes that product work? What part of the software really makes it work?’ And those are the things that we really need to protect. Some IP is more important than other IP.” At IBM, added controls protect the most important IP, not indefinitely but to give IBM a six-month head start on its competitors. Goldman Sachs has gone one step further: “We have a lot of intellectual property, but in some cases when a product is launched you have to assume that people will reverse engineer and mimic that product, at that point your ability to execute better is what counts—keeping the secret before launch is paramount but you have to be careful to focus on what needs constant protection.”

Effective provisioning is an essential initiative for IP protection: providing people with information, but only the information that they need, and revoking their access to it when they no longer need it. A frequent challenge is developing a process for removing access to information and resources when people leave the company or no longer need to use that resource. A number of attendees of our recent workshop already have processes in place for provisioning. At IBM, some of these processes are long-standing, as Betz explained. “We have a wide variety of processes in IBM. But probably the most mature is the mainframe group, where if you work on this component of this little piece of the operating system, you’re not even allowed to touch anything else. So they’ve been doing access control for probably 20-plus years in a very rigid way.”

Aetna’s Cody agreed that provisioning can be very useful, especially if it is supported by automated work flows: “To some degree, I think we’ve done a good job at Aetna with our internal provisioning. And we’ve also built some workflow automation around that so that on a nightly basis there are feeds from our HR systems which allow us to take change and basically remove access and reestablish access whenever there is a department change, a job code change, so something that indicates that the roles and the responsibilities of the organizational placement of the individual need to be reviewed.” Said Cody, “We have a lot of automated recertification for even things like network groups and network group authorizers and so forth on a semi-annual basis that helps us to some degree. This is just one example of the many, many re-certifications that we have automated through the workflow for our Sarbanes Oxley-compliance.”

Consider risk in relationships. In a global economy, firms increasingly have deep and wide extended enterprises, supply chains and partnerships that are crucial to business success. The continuing trend toward outsourcing and offshoring increases a company’s potential risk, particularly when security standards at partner organizations may be weak. As General Dynamics’ Pete Stang explained, “Clearly, that chain gets weaker with every step. And in some cases for products we’re building we have second-, third-, and fourth-tier suppliers, many of which have little to no information security. You can certainly have a non-disclosure agreement and throw the laws at them—like economic espionage or patents—but when the day’s done, your competitors are not sleeping and could get at your information through the extended enterprise.”

Many large companies interact with hundreds of small businesses, many of which simply don’t have the resources or expertise to implement strong security but which may hold important data or IP. As Cody explained, Aetna has been examining its business partners over the past 12 to 18 months to understand the level of risk they pose to the company’s data. Part of this vetting and “risk stratification” process includes an extensive security questionnaire and signed attestations regarding Aetna’s fundamental security expectations. Onsite audits to verify security measures are planned. Aetna may choose not to do business with potential partners that pose excessive security risks. Some participants offer small partner firms the opportunity to get IT service, including security, from the same IT service company they partnered with. That way, smaller firms can achieve an adequate level of security without having to build their own IT security department. As one participant at our recent workshop noted, “We gave up beating them harder and harder with bigger and bigger sticks and actually figured a way to help them. We have a security clause in our contracts with service companies that specify a certain level of security that they have to meet. The difference is that now we help them meet it.”

Another way to reduce risk is to consolidate the number of partners, each of which must meet minimum security standards. Aetna asks, “Are there opportunities for consolidation? Are we really carefully considering all of the arrangements that we have in place, and are we retaining only those that most align with our standards and have the core competencies that we need?” Goldman Sachs makes business units take into account all the costs associated with outsourcing services, including the total cost of the risk, to force economically motivated decisions. This approach has led to more rational outsourcing growth.

Because of legal and cultural differences, companies can’t “use the same looking glass” in different places. Cargill’s Gabby said, “We’re in China. We’re in India. We’re in Russia. What I’m learning is that there really are different cultural roots in different countries. We have to appreciate that cultural differences exist and that they make a big difference.” In addition, some countries have no IP laws or enforce them poorly, putting firms at greater risk. Eaton’s Matejka said: “It’s not about trusting another person. It’s about the laws in that particular country—if there’s IP theft in the U.S., you can probably get somebody into court within 2 to 3 years. In China or India, it’s not going to happen; at least it hasn’t happened with any degree of certainty. So to compensate for the weaknesses in the laws of those countries it is justified to implement tighter or stronger levels of technical control.” BT’s Nowill emphasized the risk posed by foreign governments: “When you do a risk assessment, which includes some of the problems of offshoring and outsourcing, the day-to-day risks in places like India or China are absolutely well managed. But you have a completely different set of risks at the governmental level which are impossible to mitigate by and large.”

Think like the Web 2.0 generation. Current college undergraduates are part of the Web 2.0 generation, and they think about and use technology differently from older workers. For example, the availability and power of consumer electronics means young people make different demands on employers. Many young workers have more capabilities on their home PCs than their employment workstations. And thanks to consumer electronics with numerous new applications, social networking sites, blogs, and wikis are now mainstream communication tools. With these changes come more avenues of vulnerability and risk[15]. Ramleth describes this difference: “This generation doesn’t necessarily view IT as a risk element.”

Simply banning new technologies from the workplace does not work; employees either break the rules or find a job more welcoming of their attitudes and technological devices. DISA’s Stempfley said, “It’s all about getting that kid out of high school to be willing to join the service and appreciate the fact that if you put him on a ship all of a sudden the communication that he has on his hip in high school is gone, and how do I keep him and bring him in and engage him?” Some companies address this situation by turning the tables: using Facebook and other sites to get information about job applicants.

More traditional (older) employees are learning to use these new technologies, too. Unless managed carefully, data leakage can result, as more information is flowing around environments which, by default, are more open than the business would like. Security costs can skyrocket, with deployment of digital rights management and fine-grained access controls so that the business can support innovation without placing information at risk.

Change what no longer works. Some security processes and structures no longer serve their purpose, even though they are sought by auditors and regulators. Security leaders should be prepared to make a strong case for change. Venables recounted how his company overhauled much of its security governance structure, including ridding itself of its information security steering committee, in order to “build security more into the fabric of the corporation.” At Goldman Sachs, they apply risk governance by integrating with what they call “business practices committee, which is the executive management committee that guides regulation, compliance, and business operational risk, amongst other things.” Said Venables, “We also integrated ourselves with the various business unit risk committees. So effectively we became just part of every other risk that the company regularly focuses on. It was a fairly difficult decision at the time. But almost instantaneously, after several rounds through the various risk committees, it was clear this was a first-class risk alongside all our other risks. We were finding ourselves getting much more immediate sponsorship for things and much more attention on things, bringing these newer risks to existing risk governance was more effective than creating new governance for the new risks." Cisco acted similarly in 2002, disbanding its security council because it was ineffective.

Good security sometimes requires a fundamental re-thinking of established business practices. Businesses fear that change could annoy customers, driving them to competitors. So executives can engage the marketing and sales departments to educate clients about the need for security. If clients create demand for security from the outside, internal changes to business practices will naturally follow.

Conclusion - Moving to Action

Regardless of the specific risks and challenges within a particular firm, how should firms move forward? The general elements of any program should:

- **Rank the information threats.** What are some of the largest threats in your business? How do you prioritize those threats? Do you have a process for discovering new threats and communicating risks to the organization?
- **Communicate the information threats.** How do you help the organization understand and recognize economically driven threats? How does the organization embed these risks into its overall risk management? How do you jointly educate and manage the threats within your supplier and partner organizations?
- **Measure progress.** How do you know if information risk practices are making a difference? Is the organization making progress? How should we measure improvement? What tools and methodologies do you use to do this?

However, technologies aside, information risk management must be baked into every business process. Moving the organization towards 'security at the source' means information risk must become everyone's job. The ongoing challenges of data leakage and IP protection are clearly linked to access and privileging; they will be addressed only when information risk practices become part of the organization's culture and conscience.

References

[1] M. Eric Johnson, "A Broader Context for Information Security," *Financial Times*, 16 Sept. 2005, p. 4.

[2] Working Group Members, http://mba.tuck.dartmouth.edu/digital/Programs/CorporateEvents/CISO2007.html

[3]M. Eric Johnson, "Information Risk of Inadvertent Disclosure: An Analysis of File-Sharing Risk in the Financial Supply Chain," *Journal of Management Information Systems*, Vol. 25, No. 2, 97–123, 2008.

[4] Adam Beautement et al. "Modelling the Human and Technological Costs and Benefits of USB Memory Stick Security," *Seventh Workshop on the Economics of Information Security*, Dartmouth College, June 26-27, 2008, http://weis2008.econinfosec.org/index.htm.

[5] Sasha Romanosky, Rahul Telang, Alessandro Acquisti, Do Data Breach Disclosure Laws Reduce Identity Theft?, *Seventh Workshop on the Economics of Information Security*, *Dartmouth College*, June 26-27, 2008, http://weis2008.econinfosec.org/index.htm

[6] Ross Anderson and Tyler Moore. "The Economics of Information Security," *Science* 314(5799) 610–613, 2006.

[7] Walter S. Baer and Andrew Parkinson, "Cyber Insurance in IT Security Management," *IEEE Security and Privacy*, May/June 2007.

[8] Shari Lawrence Pfleeger and Rachel Rue, "Cybersecurity Economic Issues: Clearing the Path to Good Practice," *IEEE Software*, January/February 2008.

[9] L. A. Gordon and M. P. Loeb, "Process For Deciding on Information Security Expenditures: Empirical Evidence," *Communications of the ACM* (January 2006), pp. 121-125.

[10] http://www.bitsinfo.org.

[11] M. Eric Johnson and Eric Goetz, "Embedding Information Security into the Organization," *IEEE Security and Privacy*, May/June 2007.

[12] Shari Lawrence Pfleeger, Martin Libicki, and Martin Webber, "I'll Buy That! Cyber Security in the IT Marketplace," *IEEE Security and Privacy*, May/June 2007.

[13] Bruce Schneier, "Psychology of security," Interdisciplinary Workshop on Security and Human Behaviour, MIT, June 30-July1, 2008, http://www.cl.cam.ac.uk/~rja14/shb08/.

[14] Eva Andrijcic and Barry Horowitz, "A Macro-Economic Framework for Evaluation of Cyber Security Risks Related to Protection of Intellectual Property," *Risk Analysis*, Vol. 26(4), 907-923, 2006.

[15] David Rosenblum, "What Anyone Can Know: The Privacy Risks of Social Networking Sites," *IEEE Security and Privacy*, May/June 2007.