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

Thought Leadership Summit on Digital Strategies

Security and Privacy: At Odds with Speed and Collaboration?

An Overview

Executive Roundtable Series
May 25, 2004

Cisco Systems

Security and Privacy: At Odds with Speed and Collaboration?*

Thought Leadership Summit on Digital Strategies

An executive roundtable series co-founded by the
Center for Digital Strategies at the Tuck School of Business and Cisco Systems, Inc.

Cisco and the Center for Digital Strategies at Dartmouth's Tuck School of Business recently convened the seventh in a series of thought leadership summits. This roundtable discussion focused on the impact of increased security and privacy of information on businesses, and organizational changes that would serve to ameliorate the impact. The sessions were moderated by John Gallant, the editorial director of Network World, and included business leaders and academics from Bentley College, Cargill, Cisco, Citigroup, Dartmouth College, Dartmouth-Hitchcock Medical Center, Eaton, Fidelity, General Motors, Harvard, Hasbro, IBM, Owens Corning, Staples, and the Tuck School at Dartmouth.

Key Insights:

*A synthesis article by Scott Dynes, Research Fellow, Center for Digital Strategies and Senior Research Fellow, Institute for Security Technology Studies (ISTS) at Dartmouth.

Introduction

Information security and cyber security (both will be referred to generically as information security) encompass a relatively new set of challenges that are widely shared among corporations. These challenges affect how organizations operate internally, and interact with their customers and partners. The discussions that took place at this summit addressed the important issues regarding information security in the enterprise today, and illuminated several best practices.

Information Security Is Everyone's Responsibility

Within most participant's organizations there is a prevailing view that information security is something that information technology (IT) 'does'; for everyone else in the organization, information security just 'happens' to them, their involvement is passive. This feeling can be found at any level in the organization. It is only within the core IT function of the company that information security seems to be integrated into the daily work routine and that support from senior management is generally strong.

John Cianci of IBM has experienced this prevailing view; he shared that the majority of employees possess a security buy-in issue at the ground level. John said about their attitude surrounding security measures: "I go to do my job. I don't want to spend time doing this." He also said that there is buy-in on the importance of information security from top IBM executives.

Another participant related the level of interest his board has in information security: "...when I talked about applications, their eyes lit up. When I talk about security, I see glazed [eyes]" he said.

Ken Rathgeber of Fidelity described the customer's attitudes towards information security: "...I think the general consumer out there believes that they are protected from [security incidents such as identity theft] and we will assume the responsibility and the liability of making them whole."

A major theme throughout the summit was how to make it known that information security is not just a problem to be resolved by the IT department. Everyone has a role and a responsibility for information security—even customers, as Hillary Gal of Citigroup made clear: "…customers have to understand they have to take some responsibility. Customers do not have a good understanding that what they do matters in terms of security."

Education and Cultural Change Are Key

Educational and cultural change efforts were identified as important themes in driving information security responsibility throughout the organization. One important component encompassed developing skills and capabilities and establishing a more rigorous, coordinated approach to information security. Other elements focused on building awareness of individual and collective responsibilities, getting people to move from observing information security in a passive role to seeing themselves as an active player on the corporate information security team.

It was agreed that awareness-raising and educational efforts should begin at the board level. Both Robert Austin of Harvard Business School and Jim MacDonald of Fidelity voiced that information security was going to be a major board issue, and that chief information officers (CIOs) needed to educate the board about information security issues. Robert Austin: "WorldCom turned out to have no one on their audit committee that was an accountant or had expertise in accounting… Is security really any different? Shouldn't the board have an obligation to understand this issue that's got such high stakes?"

Participating executives also expect their customers to take responsibility. Echoing Hillary Gal's earlier comment about customers, Ken Rathgeber of Fidelity related how Fidelity will begin informing clients that if they haven't installed a certain level of web browser on their computers, they won't get access to Fidelity's secure web site.

Though board and customer education were seen as important, most of the education and awareness efforts discussed were directed towards corporate employees and extended enterprise partners. Many of the ideas discussed were aimed at educating workers on their responsibilities and roles in the organization's information security efforts. For example, companies are starting to take a more rigorous approach to educating the workforce during new employee orientation, and adopting yearly sign-offs on corporate information security policies as a way of reinforcing corporate policies.

Scott Day of Cargill related how their organization is embarking on information security training/education by roles. "We've identified what the roles are, the business unit leaders are in there as well. What does the business manager need to know? He doesn't give a rip about TCP/IP but he needs to know how it affects his decision rights... We've taken that on because we think that's something that will help internalize it into the culture. When everybody knows what it is they are responsible for and how they are going to be held accountable, then they can go get what they need and make sure they are up to speed on it."

Max Ward of Staples felt this more nuanced approach is important: "I agree with Cargill's approach to [look] at not just educating masses but the fact that you've got to look at the role people play and understand what it is they need to know based on their role...To me, it's almost worthless doing this [if you are just doing] awareness training or just giving the same level of information to everybody."

More than one participant indicated that external audits helped drive organizational education. Scott Day related his experience: "I can give you an example of how an external report … got us into action … we spent about 70,000 resource hours in just doing those five activities across the world… It's gotten people to understand a bit more about their risk profile and the business they are in and the roles in relationships they have with everybody else. It's pervasive. They are getting a good head dunking in the information security when they are in the field."

Organizational and Cultural Change

While education was seen as an important initiative, time was also spent on how to ingrain information security into the organization in other ways.

Scott Day at Cargill on enabling the cultural aspects of information security across 85 business units and functions: “We tried to link it to the familiar cornerstones of things that they do daily and it has worked out pretty well so far. We are a long way from where we want to be but we are starting to get the momentum it needs.” Andrew Gottschalk, also of Cargill continued: “It turned out that early on some of the worst violators were in the executive offices. I think this was a wake up call to some of these people that this is important and that's something that you need to take personally. Some of that personal ownership has really helped allow Scott to be effective even with a real decentralized environment.”

Chris Dunning of Staples and Ken Rathgeber of Fidelity echoed this theme of tying information security to critical business cornerstones. Chris Dunning: “Trust is the message that we used to drive change in the technology organizations… [our employees] know that our customers trust us to keep their data secure. Our stockholders trust us to put the right controls in place...”

As part of the discussion around embedding information security, participants discussed what happens if employees don’t change and conform to information security policies. John Moore of IBM talked about IBM’s approach: put simply, if you don’t comply, you’ll get burned. People learn from that. Tom Sanzone of Citigroup told of a technique they use: web-based information security performance models and scorecards listing all out-of-compliance issues and a timeline for resolution. Managers see this when they log in every day. Sanzone related that there have been some high-profile instances where failure leads to economic consequences for employees, “and people know that.”

Brad Boston described Intel’s creative idea of handing out “traffic tickets” for information security violations. Unexpectedly, the violator’s manager is the one that pays the fine. This involves the manager and their group in corporate information security practices. Other examples of the information security “stick” include direct impact to worker’s bonus, and calls from the “big boss” regarding an information security breach.

Information Security Should Be Decided By...?

One organizational challenge was talked about in some detail—the tension between IT and business with respect to information security. These natural tensions arise from the dual and sometimes competing needs for increased security and enhanced collaboration and business speed. How are these competing forces resolved?

Brad Boston of Cisco shared an example of this tension and its resolution: If a business unit wants to do something unique, the business unit executive will sit with the information security group. This group used to have the authority to say ‘No’ to business unit requests, which they did all the time. Boston intervened: “We said your job is to identify the risk. The threat of that risk actually occurring, the probability and tell us what the options are to remediate it. Then a business decision is made about what risks are acceptable and which risks are not.”

Hillary Gal of Citigroup related a similar situation inside of Citigroup, where information security was largely driven by IT, which has little contact with the customer-facing side of the business. Citigroup created a new role to ensure greater visibility of business issues in information security, to work on getting business driving information security into all the businesses rather than “something that IT continues to tell you that you have to do.”

Eric Johnson of Tuck elaborated the uncomfortable part of the tension for the CIO: the basic instincts of a security executive center around policing, saying no; the instincts of a good CIO are enabling business and working with the executives around strategy, and yet the information security function usually resides under the CIO. Some corporations are resolving this by creating a CISO (chief information security officer) role which often does not report to the CIO—that is the case at Fidelity, for instance.

There was a general agreement that business needs should be the main driver; as Max Ward of Staples put it, “I never want to be in a position that the business wants to do something and I'm constraining it.”

Culture Clash: Attitudes of Future Workers
There was an interesting thread about the difference in cultural norms between university students and the corporations for which they will be working. Peter Johnson of Dartmouth-Hitchcock Medical Center: “One of the things that you have to understand is that today's students are tomorrow's employees.” Regarding student’s attitudes about the PC they use: “...this is my thing, you can't touch it and that's a very hard culture. We [corporations] all think of these things as these are our business instruments.” Denise Anthony of Dartmouth related that 75% of students share passwords.

Such attitudes (and the availability of broadband at workplaces) might explain the abundance of mp3 and mpeg music and movie downloads; it was pointed out that the presence of pirated files on corporate machines is a legal liability for that corporation.

Denise Anthony held out hope: “[The Computer Science field] used to be encouraged to train students to hack as a way of highlighting vulnerabilities and that kind of thing. That has completely shifted. There is real training and discussion of the ethics of that and if you're going to be a good guy now, it's not to figure out how to hack in.”

The Quality Analogy—a Six-Sigma for Information Security?
The themes raised in the discussion around information security reminded Eric Johnson of Tuck of the quality initiatives that business experienced 20 years ago. He wondered about the analogies between the quality effort and the information security effort. The conversation at that time centered around the cost of quality, the importance of quality benchmarking, whether the level of spending on quality was appropriate, and what the return on investment was. The quality issue was about driving quality practices down to the lowest level of the organization, the notion of taking it from the quality control departments and driving it down to the individual workers and processes. An analog for information security would involve the integration of information security practices into the daily work of everyone and every entity in the extended enterprise. Information security methodologies would have to be built into the

organization, the process and the product, rather than being bolted-on at the end. Participants of GM and Tuck were interested in what we could learn from the quality analogy that would inform their current efforts.

Balancing Risks and Security Through Sharing

How can organizations best determine the risks they are exposed to, both now and in the future? What are appropriate actions to take to mitigate those risks? The following issues kept some of the participants awake at night.

Executives described a range of methods used to define the risks, and to prioritize those risks. For example, Jim MacDonald of Fidelity talked about a cyber threat matrix—a four-quadrant matrix plotting the likelihood of an event along one axis, and the impact of an event on the other axis. "…The top right quadrant is our best analysis of what requires immediate attention and senior executives should focus on," he explained.

Don Kosanka of Owens Corning also talked about the information risk/security balance: "We use a similar process to what our manufacturing plants think about when they think about liability. When you look at a manufacturing facility, you try to understand the probability of a failure and the impact of that failure. Looking at those two factors, [you make] decisions about how much you're willing to invest given the probability of something happening and the impact of it happening." (For more details on risk/impact-based approaches to information security see *How Much is Enough?* presented by Kevin Soo Hoo at the 2002 Workshop on Economics and Security. It is available at http://www.cl.cam.ac.uk/users/rja14/econws/06.doc).

In this approach the issue is thinking about what might happen that you have not seen before, about what might come next that could be very damaging—"blue-sky thinking", as Jim MacDonald puts it. This is hard. Don Kosanka added, "That's the part that's not exact science. You have to make predictions. You have to make guesses based upon what happened in the past and what you're hearing about in the future."

Information security risks could arise from within the organization, a point that many found concerning. Kosanka said Owens Corning's applications were developed for use in their factories when the factories were isolated from the outside world, and information security was not a design concern. Such manufacturing applications, being tied to the business applications, significantly increase the potential for vulnerabilities in networks.

John Cianci of IBM also worried about internal risks in the form of servers in IBM's labs that are not as closely managed; he discussed a capability to separate a lab with infected servers from the rest of IBM's network to mitigate that risk. Brad Boston of Cisco has faced this situation as well: "We had to isolate all the labs. They were my biggest source of denial of service attacks."

Another potential security breach for companies is via employees who connect to internal networks through broadband connections, or with wireless networks at their home that might be accessed by anyone on the street. Employees who bring in personal devices such as laptops, PDAs and Blackberries, or who mingle personal and corporate data on such a device were also identified as sources of risk, both from an information security standpoint as well as an employee privacy standpoint.

Information Sharing

To assist with risk identification and mitigation efforts, many participants voiced their desire to find a way to share experiences about information security. Tom Sanzone of Citigroup: “One of the things I think would be helpful is reporting our incidents on a blind basis to some kind of a group that consolidates this information and then feeds back what's going on in the business, what are the incidents, what are the highest probabilities and the exposure.” Robert Austin of Harvard agrees, and makes an argument for sharing through third parties: “… For example, a third party knows that the attack you suffered this morning is also being experienced by ten other companies. It does strike me that there is a natural role for some sort of an outsourcing partner to play in the security. They can compile more data. They can help you benchmark.”

While many were eager to participate in such a system, most thought that anonymity issues would in practice be difficult to overcome. Eric Johnson of Tuck related that he had been talking to a retail company about sharing similar kinds of information with an industry consortium; that company was not interested because of possible damage to their brand. Others were more hopeful. Tom Sanzone of Citigroup: “We share our compensation information with third parties that do comparisons. So if we're willing to do that, I think we'd probably be willing to do this. It depends on the environment.”

A few participants told stories of how external evaluators were able to provide some of the norming information. Chris Dunning of Staples: “The approach that we took is we brought in a third party to perform a security benchmark. They had the statistical data within our industry that said this is basically where you should be from the best practice point of view...What they were able to tell us is what are the other 50 largest retailers in this country doing? Where do you position that? That enabled us to put together a program and a plan that went out five years.”

There are existing groups that were formed for this type of information sharing: the Information Sharing and Analysis Committees (ISACs). ISACs exist in many business sectors, and could serve the role outlined by Tom Sanzone above. In a recent government-sponsored information security exercise run by Dartmouth, the Financial Sector ISAC (FS-ISAC) was an important mechanism for the financial industry to share anonymous information during crisis situations.

Regulation Is a Blunt Instrument

Participants had very aligned views about government regulations (e.g. Sarbanes-Oxley and EU privacy regulations): participants felt that regulations frequently focused on the wrong issues, and were often inconsistently applied.

One emergent theme from the group was that the regulations written by the US government to assure accountability and protect information (such as Sarbanes-Oxley) were ineffective, focusing on the wrong issues. Brad Boston of Cisco summed up this theme: “None of these controls will prevent Enron or the next WorldCom because it has nothing to do with what happened.”

Robert Austin of Harvard Business School thought the job facing regulators was very challenging, that there was a "fundamental knowledge asymmetry" between what practitioners and regulators knew and could act on or regulate. He related a concrete experience about auditors and auto assembly plants: "Any one of us could have thought of 120 ways…to shut plants down if we'd been inclined to. When the auditors would come through, they would ding us for things like a nonstandard browser and we laughed about it. If they even identified 10 percent of what we could do to them, we'd be staggered."

Participants were also exasperated by the lack of predictability and uniformity when dealing with Sarbanes-Oxley, both in terms of what is required to meet the regulation, and in how those requirements are interpreted by auditors, who also are responsible for meeting the regulation.

This lack of standardized interpretation led Doug Schwinn of Hasbro to describe Sarbanes-Oxley as an "onerous process". "The goal line keeps changing", he said. Max Ward of Staples: "[it's like] nailing Jell-O to the wall." Schwinn solidified Ward's comment with an example of his own: "We had documented that we did [a particular] test but then the auditor says prove to me that the document is authentic. How do we do that?"

Participants were also concerned about privacy and information security regulations in other countries. Privacy regulations seem to differ widely across EU countries. Doug Schwinn told of how it's illegal for Hasbro to know what data is traveling across their network in Germany. John Cianci of IBM related how Italian privacy laws mean that you cannot send email to a customer unless they opt in: "If you don't know about it, your chief officer in Italy is going to jail."

Michael Elliott of Hasbro summarized the impact the interpretation of EU privacy and information security regulations has had on his business: "It was an EU directive at one time and then was variously interpreted by the national governments. When you go to Italy, you got the problem that John just described. If you go to Holland, and you send spam out, you can actually go to jail. You need interpretation across all European countries when you get into that consumer market. That certainly is slowing us down."

U.S. companies have also been paying more attention to the appropriate use of customer data. To help prevent inappropriate use of customer data, Fidelity erects "Chinese walls" between business units so that one unit has no access to the customer data of another unit. Michael Elliott explained that Hasbro has a policy where there is one owner of all data that is held on behalf of consumers. That owner is responsible for assuring that any use of customer data is in accordance with Hasbro's customer privacy policies.

Information Security Is Impacting the Extended Enterprise

It is clear that information security is not just impacting corporations, but also those corporations' extended enterprise. Within individual corporations information security is affecting mind share; across corporations information security is affecting the speed of business and of developing partnerships, or even whether these partnerships will be formed at all (see the **Information Security: Good For Business, but For Competition?** section below for a view of how information security can potentially make for better partnerships).

Within the enterprise, issues such as fire-fighting the latest virus and patch management were regarded as major issues both from a cost standpoint as well as a mind-share standpoint. Tom Sanzone of Citigroup highlighted how employee time spent on such maintenance issues results in lost opportunities for value-added services. Jim MacDonald of Fidelity echoed this theme, talking about how high-level workers spent time patching machines to fend off the latest virus rather than thinking about business strategy and competitive advantage.

Information security issues are also delaying the work of contractors and employees who travel. Contractor work is delayed because of assuring that contractor's machines meet information security guidelines for patch levels and other information security methods. On-the-road access by employees from hotels via broadband, Blackberries, etc. is also impacted by information security concerns.

There were many examples of information security impacting how corporations are interacting with each other as well—a point Mary Culnan of Bentley College raised when she wondered about what shared information security responsibilities companies have to each other. To address this issue, participants are auditing the information security status of potential partners, which slows down partnering and supply-chain relationships.

John Moore of IBM explained: "…you really want to be able to tie two networks together to have that free flow of information but if company A doesn't have the same standards or security standards, guidelines or policies that your company has, then you're really opening up your door to everything that wants to come in. You just have an animal swing door there; it [network traffic] comes and goes as it wants."

Doug Schwinn of Hasbro: "As we extend the enterprise out to the suppliers, having to deal with security and validating that this guy is trusted and how we get through that process, it is slowing that process down but we have to do it. There's just no way around it."

Brad Boston of Cisco added, "I've talked to some very big-name companies that are totally clueless. They are working on last year's problem, not today's problem and not even thinking about tomorrow's problem. If they are right in the middle of your supply chain or your eco system, you're hugely vulnerable from their inability to be able to respond."

Mark Hillman of GM also sounded a cautionary note about assuming anything regarding the information security practices of business partners: "I would encourage anybody, if you do a lot of outsourcing, you need to go poke at everybody…" GM has a set of guidelines he requires vendors to adhere to; GM audits partners to assure compliance.

The above examples depicted how security measures might hinder progress. Jim MacDonald of Fidelity described how information security issues has affected innovation in his company: "Working with small technology companies, terrific innovative systems, is an issue for us in that we tend to like those companies because they can help us get a competitive advantage. When we go in and do security assessments, it's usually not been an area of focus for the company and may be lacking somewhat. We've gone slower creating partnerships with those types of companies that we're not happy about because we see the technology and it's terrific but they just don't have enough [information security] emphasis.”

Information Security: Good For Business, Yes; but For Competition?
Is information security a competitive advantage? Does it have a positive business case? The disposition of the group was that while better information security would not confer a lasting competitive advantage, companies that paid close attention to information security would benefit from both direct and indirect outcomes of information security efforts.

Robert Austin of Harvard Business School captured the mood when he cast the question in terms of whether information security is “compete vs. qualify”: Is better information security worth more, or do you have to have a certain level to even play the game? Reinforcing this view, many people held views similar to Eaton’s Jack Matejka: “Failure in security, that [is what] gets noticed. If you're successful, it's expected.” Mark Hillman questioned whether touting better information security could even be a disadvantage: “Those good housekeeping seals out there, that just raises the question for the consumers.” Do airlines use how few crashes they’ve had as a selling point? Ed Kriete of Hasbro summarized the issue well: “If you screw it up, there's going to be a real consequence, but at this point, it's really a qualifier.”

While most thought information security might not be a sustainable competitive advantage, many felt that there existed a positive business case for better information security. Tuck’s Eric Johnson made the case: “A lot of things that are related to securing your company aren't technical things. They're operational things like being very disciplined in change management and things like that. If you really focus hard on operations with an eye to improving it, you almost always realize multidimensional benefits from that, not just one dimension.”

Mark Hillman of GM gave an example showing the beneficial consequences: “…I'd say in retrospect, it's been a more important thing than you probably would realize. Going into it [more rigorous information security practices], we started finding out how far behind things are or plant level issues that are very serious…risks.”

Max Ward highlights how Staples is succeeding: “We're taking market share from our competitors right now. One of the reasons for that is because we can answer the question that we are going after new business that says ‘how are you to guarantee the system is going to be there when I need it.” Staples’ better security gives it a direct competitive advantage by raising the customers’ confidence in Staples’ ability to deliver.

Hans Brechbühl of Tuck posited a supply-chain example: “What about the idea that there is some system that you may be putting in for the purpose of security that could actually be used to enhance supply chain visibility? In that sense, really, you would have a very positive business case... Say I'm spending dollars in security because not only am I getting better security, I can also get better visibility on all my goods being shipped from Asia or wherever that may be.”

John Moore of IBM had a story that also supports this view where security renders an indirect form of competitive advantage: “We are applying some devices on our network today that were intended to stop certain types of traffic and we have quickly discovered that we are gaining the benefit of visibility, seeing things on the network. Now we're beginning to see patterns. Had we been more proactive, we could've been catching [this] all along. We're beginning to gain the capability of usage-based billing. You use this much of the network, this is your portion of the bill. So we are starting to see the by-product of the benefit of deploying this stuff."

Conclusion

We are at an early stage in the evolution of information security. This is clear from the largely reactive manner in which information security issues are dealt with, the lack of transparency regarding the types and effects of attacks on organizations, even the lack of an accepted framework in which to think about, plan for, and share information about these issues.

The types of information sharing that occurred at the summit are the key to the development of such a framework: everyone has a piece of the big picture they can contribute, and it is only by seeing the big picture that we can move from being reactive to being proactive, move from wondering about unknowable threats to a more quantitative, reasoned approach to information security. The development of this framework will also make clear what roles organizations and governments play, and what responsibilities organizations have as "good internet citizens".

This informed, emergent approach would certainly to be preferable to the most likely alternative: a major information security and/or privacy "train wreck" that will certainly lead to a call for greater regulation of information security and privacy, which will neither be effective nor pleasant.

There is no doubt that effective information security processes will become part of the paradigm, much like quality processes are now. Getting to that point will be a long road of questioning current practices, adopting new ideas, developing new social networks. Defining the issues and developing a framework for looking at them is an important start.

Participants in Thought Leadership Summit on Digital Strategies
May 25, 2004

Denise Anthony	Assistant Professor of Sociology Dartmouth College
Robert Austin	Assistant Professor Harvard Business School
Brad Boston	Senior VP and CIO Cisco Systems Incorporated
Hans Brechbühl	Executive Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
John Cianci	VP, Global IT Infrastructure IBM Corporation
Mary Culnan	Slade Professor of Management & Info. Technology Bentley College
Scott Day	Global Information Protection Manager Cargill, Incorporated
Chris Dunning	Director of Enterprise Security Staples Incorporated
Michael Elliott	Head of IS, Europe Hasbro Incorporated
Hillary Gal	Managing Director, Head of Technology Control Citigroup Global Corporate and Investment Banking Group
John Gallant (Moderator)	Editorial Director & President *Network World*
Andrew Gottschalk	Attorney Cargill, Incorporated
Mark Hillman	IT Director, Global Supply Chain and B2C Operations General Motors Corporation

M. Eric Johnson	Director, Center for Digital Strategies Professor of Operations Management Tuck School of Business, Dartmouth College
Peter A. Johnson	CIO Dartmouth-Hitchcock Medical Center
Don Kosanka	VP of Information Systems Owens Corning
Ed Kriete	VP, Marketing Services Hasbro Incorporated
Jim MacDonald	CIO Fidelity Management and Research
Jack Matejka	Director of IT Security Eaton Corporation
John Moore	Director of Extranet and Intranet Security IBM Corporation
Ken Rathgeber	Executive VP & Head of Risk Oversight Fidelity Management and Research
Tom Sanzone	CIO & Managing Director Citigroup Global Corporate and Investment Banking Group
Doug Schwinn	Senior VP & CIO Hasbro Incorporated
Max Ward	VP of Information Technology Staples Incorporated