TUCK SCHOOL OF BUSINESS AT DARTMOUTH
GLASSMEYER/MCNAMEE CENTER FOR DIGITAL STRATEGIES
www.tuck.dartmouth.edu/digitalstrategies

I3P
Institute for Information Infrastructure Protection

Security through Information Risk Management

A Workshop for Information Security Executives

Security through Information Risk Management[1]

A Workshop for Information Security Executives
Hosted by the Institute for Information Infrastructure Protection (I3P) and the Tuck School of Business's Center for Digital Strategies, both at Dartmouth College

A workshop for information security executives convened to discuss how companies are shifting their mindset from information security to information risk management —particularly risks due to specific economically motivated threats. While security professionals have long talked about risk, moving an organization from a "security" mindset to one that thoughtfully considers information risk is often a challenge. Managing information risk means building risk analysis into every business decision. This report explores how security executives are moving the conversation toward risk, how to help organizations categorize and communicate risk, and how progress can be measured. The workshop included security leaders from 3M, Adidas, Aetna, Bechtel, BJ's Wholesale Club, Bose, BT Group, Cargill, Cisco Systems, Colgate-Palmolive, CVS, Dell, Dow Chemical, Eaton, Eli Lilly, General Dynamics, Goldman Sachs, Hewlett-Packard, H&R Block, IBM, Staples, Time Warner Cable, United Technologies and the U.S. Department of Homeland Security and DISA, along with academics from Dartmouth, RAND, and the University of Virginia.

Key Insights Discussed in this Article:

---

[1] This overview was written by Eric Goetz of the I3P and Professor M. Eric Johnson of the Tuck School of Business at Dartmouth College. The workshop and research 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.

Information Risk Management

As information security risks continue to evolve, many organizations are moving from a traditional security mindset to a risk management mindset. Effectively evaluating the risks, both internal and external, requires understanding the motivation of the attackers. While shielding the organization from the latest worm or viruses may consume many security resources, the most serious threats to any business come from attackers with economic motivation. Increasingly, organizations are faced with threats from professionals with very specific motivations. Some of these motivations are obvious and immediately recognizable. Others are more subtle with lasting impact. For example, protecting against intellectual property leakage may be one of most difficult assignments for CISOs since the losses are often not immediately observed and the impact may not be felt for years. Protecting against these economically-driven threats requires much more than technology. It requires building security into the culture so that everyone can recognize and evaluate the risks.

The workshop examined many aspects of information risk, touching on issues like ranking and prioritizing risks, internal communications and measuring security progress. Throughout the day, senior security executives debated risk management and security issues. The focus of the workshop was on peer-to-peer learning enabled through moderated discussions. The goal was to learn from each other and to be able identify some best practices and bring to the forefront the most innovative ideas concerning moving security into the mainstream of corporate risk management.

Workshop chairman Eric Johnson from the Tuck School of Business and the Center for Digital Strategies opened the workshop by asking participants to identify their most pressing current risks, as well as future risks approaching on the horizon. The following are the most pervasive risks the group currently faces:

- *Protecting intellectual property.* The leading risk identified was the potential loss of a company's intellectual property (IP), which, in a knowledge economy, is increasingly the lifeblood of a company. While the protection of IP requires the effective use of technology, a key component is also the human element. User awareness and education are critical to ensure that employees understand what IP is, how valuable it is to the company, and who actually owns it (i.e., that the company owns the IP and not the individual employee). Geir Ramleth from Bechtel explained the problem: "You have to actually teach people 'who owns the intellectual property?' I don't think the main problem with intellectual property is a technical challenge. 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?" A major challenge identified by several participants was the difficulty of adequately protecting IP in emerging markets or while doing joint ventures with possible competitors. John Brenberg from 3M said that one of the strategic initiatives that they have is "to push more of our supply chain out where the emerging markets are. So we have a lot of growth in some pretty emerging countries, and one of the areas that we talk about the most is how do we put our arms around that as we grow." Robert Nowill from BT was speaking for many participants when he said: "The things that keep me awake at night have to do with offshoring and outsourcing." Some of the main problems with IP protection in emerging markets relate to different, weak or poorly enforceable IP protection laws, as well as different cultural attitudes toward IP in some countries. Finally, just expanding the size and complexity of the supply chain can create more potential points of risk for corporate IP.

- *Data leakage.* Closely related to the IP issue, many firms are worried about data leakage more generally, especially in the context of the recent spate of reported data breaches that have had negative effects on companies' reputations and brands. Since electronic data is so easily copied, moved and transferred, data leakage is a complex problem that can occur at various levels—at the network, at the desktop, via e-mail, through laptops and handheld devices, via back-ups, or

through other technologies. General Dynamics' Pete Stang remarked, "It's tough trying to enable business at the same time as trying to prevent data leakage." Time Warner Cable's Nancy Wilson gave a good insight into the scale of the problem at some organizations: "We have about 10,000 laptops we're encrypting now, or trying to encrypt. And [without encryption, the risk of] data leakage is huge."

- *Maintaining security while outsourcing to third parties.* Also related to the protection of IP is the issue of trying to maintain internal security standards when outsourcing or offshoring work to third parties, often based in emerging markets where the legal and cultural problems described above may apply. This is an especially tricky challenge for government contractors or firms in certain regulated industries because they are bound by very specific rules and guidelines that are often challenging to transfer into a new distant environment.

- *Compliance.* Several of the retailers in the group expressed concerns about to the risks arising from the need to comply with payment card industry (PCI) standards. Others were concerned about the risks and challenges surrounding remaining in compliance with other government regulations, such as the Sarbanes Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA). The challenges of compliance are not limited to financial transactions. 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 all regulations for Blu-ray and other technologies. So I have compliance all the way down to the manufacturing floor." Some firms have to navigate a jungle of different regulations, as Jeff Sherwood from H&R block emphasized: "We're also very regulated since we have a banking product, GOPA, which is self-insured. We are subject to HIPAA and Sarbanes Oxley. We also have a regulation, IRS Reg. 7216, which is something that's directly for taxpayer information and what we can and cannot do with our offshoring."

- *Raising the bar for security.* Companies that are not at the cutting edge of cyber security, or that are not in industries that are heavily regulated or audited, were worried about keeping their security programs current and focused. At some consumer products companies or manufacturing firms, security may not always receive adequate attention and support from senior management, which could result in certain risks being overlooked or not adequately addressed. 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."

- *Staying secure as a growing global company.* As companies expand and diversify their operations and locations, the growing challenge is to maintain security from the center to the periphery. As new locations are established, the complexity of securing the business increases, and the main challenge becomes keeping the entire business on a high security baseline. Staples' Chris Dunning shared: "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, and drive from a global point of view."

- *Securing companies at the speed of business.* Many participants felt that their security programs were relatively mature and effective, but that risks arose when security tried to keep up with the accelerated pace of business activities. In many cases, companies need to rapidly pursue business opportunities, such as partnerships, third party relationships or mergers and acquisitions, and they expect security to move at the same speed. This expectation can cause difficulties for security as Linda Betz from IBM explained: "I think you have to be really fast. 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 seconded 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 a slightly different challenge: securing distributed fast-paced operations that need to function effectively for a short period of time. He noted, "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.* As firms increasingly recognize the importance of information and systems security and implement protective measures, they sometimes encounter opposition from customers or partners that don't yet see the importance of security. This can create tensions between the business priority of getting things done and the objective of conducting business securely.

Business Risk and Information Risk

A senior executive panel, made up of Geir Ramleth, Senior VP and CIO of Bechtel Group; John Stewart, Vice President and Corporate Security Officer of Cisco Systems; Phil Venables, Managing Director and Chief Information Risk Officer of Goldman Sachs; and Greg Garcia, Assistant Secretary for Cyber Security and Telecommunications for the U.S. Department of Homeland Security (DHS), discussed the latest security trends, including efforts to transition from a focus on information security to risk management. The panel, moderated by Eric Johnson, also focused on how companies think about security risks in relation to other business risks; the changing nature of security threats; the changing nature of protection in the context of the Web 2.0 generation; and using security to enable and drive businesses.

Creating market incentives for companies to improve their security posture. The panel raised some important questions about how to develop new ways to incentivize good security behavior. There are currently no significant market-based drivers for improved cyber security, often leaving security executives to fight internal battles to make a business case for security. In the current landscape security is primarily viewed as a cost, and not as a differentiator or opportunity. Could those entities pricing risk—credit rating agencies, insurance companies, banks that provide loans, and traders of financial instruments (risk appraisers)—create real, measurable economic market incentives for better security by developing a transparent, accurate and consistent methodology for incorporating cyber security risks into overall risk calculations, and pricing risk accordingly?

DHS' Greg Garcia stressed the need for the creation of a common reference for characterizing and pricing cyber security risk that is actionable in the marketplace. This form of cyber risk-based pricing is already starting to happen in the credit rating and insurance fields because it's a win-win situation for both sides. Those pricing risk want to minimize risk exposure by having information that's as accurate as possible about a company's risks. Since cyber security risks are potentially high-impact, being able to assess these risks more accurately in an overall risk portfolio reduces exposure to unexpected losses, and helps price risk more effectively. On the other hand, this approach provides clear standards and transparency for companies. 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. They also know that competitors who spend less on security will have to pay in other ways.

When it comes to risk transparency, the panel felt that clear and consistent standards would undoubtedly facilitate the effective functioning of market forces to accurately price cyber security risk. Garcia explained how he intends to push this initiative forward: "Right now, security is not a publicly valued market driver. In the next year or so that I'm with this administration, I want to look at where are the market-based incentives that will get CFOs to sit up and pay attention. A lot of this is going to come to down to how companies report their information. How do companies assess themselves, such that we've got measurable data that gives the market drivers in this economy an indication of your level of risk, and, therefore, your level of attractiveness in the marketplace?"

Goldman Sachs' Phil Venables described an initiative within the financial industry to make risk more transparent in business terms. Several financial firms are working with one of the leading credit rating agencies, Moody's, on a program to start doing information risk ratings of companies. Firms would use those ratings to decide which service companies they want to work with and how much they are willing to pay for various services in light of 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."

Changing things that no longer work. Security is such a fast-paced, ever-changing environment that changing processes and structures that no longer serve their purpose is essential. However, this is sometimes counterintuitive for firms where established structures provide continuity in other areas.

Changing established security structures can also cause difficulties with auditors and regulators who look to certain structures to ensure that security is being addressed. When change becomes necessary, security leaders should be prepared to make a strong case to explain the need for change. Venables recounted how his company overhauled much of its security governance structure, including getting rid of its information security steering committee in order to "build security more into the fabric of the corporation". The idea was to embed security more strongly into the overall risk management structures of the firm: "At Goldman, we apply risk governance by integrating with what we call our business practices committee, which is the executive management committee that guides regulation, compliance, and business operational risk, amongst other things. We also integrated ourselves with the various business unit risk committees. So effectively we became just part of every other risk that the company focuses on a regular basis. 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."

John Stewart explained that Cisco had taken similar action back in 2002, disbanding its security council because it was ineffective. Said Stewart, "I sat in on a meeting of the security council. We did a lot of presentations, took absolutely no action items on what to do next. And everybody got ready to leave the room and go, 'Great meeting.' I just sat back and said, 'What decisions did we make with this many people in the room?' We disbanded that group the next month."

Using the language of risk instead of IT jargon. Business executives can easily be overwhelmed or confused by the use of technical IT security terminology. This can lead to them not understanding the severity of a problem or the potential risk that problem may pose to the firm. Members of the panel agreed that moving away from using the language of IT security and, instead, adopting the language of

business risk had helped them to better articulate IT security risks. Venables reinforced that language is very important when trying to reduce security risk: "We 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."

Geir Ramleth from Bechtel agreed that language is crucial in achieving results. Senior managers at Bechtel are familiar with the concept of risk, but the risks that they can easily associate with are not cyber in nature. Therefore, the key is to put the risk conversation in terms that they can readily understand and relate to their overall goals of executing on projects in a timely fashion and on budget in difficult circumstances. "Talking about risk to our senior managers, that is very, very easy," said Ramleth. "They know what risk is. It's just that it's not information risk. So 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."

When it comes to talking about security it's also important to show the rest of the organization that security is a business enabler, and not an impediment to the work of the company. Demonstrating security as an enabler is really an internal marketing effort, whereby security leaders have to reinforce how difficult or risky projects only worked because security was built into the initiative. In general, participants were interested in exploring further how to look at security more in the context of overall risk using the language of risk management.

Convincing people to change the way they are doing business. According to the panel, one of the biggest impediments to improving security is the established, traditional way of doing business. Companies develop a mindset about how business should be transacted and it is very difficult to implement change into this process. The problem is that good security sometimes requires a fundamental re-thinking of established business practices.

One of the main difficulties is that established practices are what customers have come to expect. Business units fear that changing these practices could annoy customers, driving them into the arms of competitors. Venables recounted discussions where the direct cost of improved control has been less of a debate than the potential customer impact (positive and negative) of adopting broader controls. The impedance mismatch between the corporation and the client is paramount; any uplift in controls needs to carefully factor and support the business processes in place—and sometimes the need for them to evolve.

The panelists suggested that one way to approach this problem is to partner with the marketing and sales departments to educate clients about the need for security. That way, clients create demand for security from the outside, which can help implement internal changes to business practices. Such a proactive approach promises greater success than simply requiring secure behavior. Security requirements or controls may be ignored or resisted if they are perceived as impeding the business.

Balancing information risk against other risks. Information security risk is just one of the numerous risks companies face. Therefore, security must compete with all these other risks for attention and resources. Finding a balance between all these risks, while still operating profitably, can be a challenge for companies. This can be especially true if a company operates in dangerous physical conditions, where more tangible risks than cyber risks may prevail.

Ramleth explained that Bechtel often runs massive projects in very challenging locations: "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 often operate just

like the DOD. 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. My bottom line for risk is: it's hard to get the right balance between security and risk. It's hard to get it to a more manageable level." Making those risk decisions is the job of senior executives. Security leaders should be in a position to provide senior executives with information about threats, risks and potential consequences. Senior executives should then be the ones who make the decisions about how to balance the security risks against other risks that the company faces.

A company's security posture may also depend on its willingness to accept risk, its risk posture. So, in some cases, a company may choose not to do certain things related to security because it is willing to accept the risk that comes with the decision. However, the panel emphasized that decisions based on risk tolerance should be made consciously and be based on solid information, rather than by default or out of intuition alone. John Stewart explained that Cisco is such a company with a high risk tolerance: "My executive team, all the way to the top, is willing to listen to information risk management and also hear the words that Cisco is a high risk-taking company, which we are. In the latest examples of this, 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. The thing to remember and most of the reason to do this is because we've got shareholders that 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."

Making security a data-driven discussion, not an emotions-driven discussion. Several of the panelists have started using data and league tables to hold business units accountable for their security. The notion behind this approach is to have actual data drive decisions, instead of emotions or news of the latest security incident. This approach of creating security league tables for business units is not meant as a punitive measure—the purpose is to raise awareness of security issues and to motivate executives to improve security within their groups. Executives whose organizations are at the bottom of the rankings are always warned ahead of time and are offered assistance to fix the problem. Stewart from Cisco explained how it's done at his company: "Every Friday morning, 35 of my executives get a voicemail briefing. They get a voicemail briefing from my team on the last seven days around information security events of some type. 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."

One of the goals of using lists or league tables to identify security underachievers is to motivate employees and executives to become more proactive about security. The people that end up at the bottom of the rankings take security much more seriously, but, hopefully, that experience also motivates everyone else to actively improve security measures in order to avoid being the next 'victim'. As Rodney Baker from Adidas put it, "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. But it has to be more than education to become the human nature that it is of showing up as a red light."

Impact of Web 2.0 and the Web 2.0 generation on businesses. Current college undergraduates in their late teens and early twenties are part of the Web 2.0 generation. As this generation enters the workforce companies will have to adapt to their use of technology and the potential risks that brings with it.

One major change has been the availability and power of consumer electronics—it used to be the case that people could do much more with the technologies that were available to them at work. This has changed to the point that it has been reversed and most people have greater capabilities on their home PCs. In addition, consumer electronics are widely available and numerous new applications, such as social networking sites, blogs, wikis, etc. have emerged as mainstream communication tools. These changes have created many more avenues of vulnerability for companies and have also changed the mindset of employees and technology users in terms of risk. Ramleth from Bechtel summarized the trend well: "The attitudes of the Web 2.0 generation toward all these technologies are different to ours—I think they will start putting different demands on the corporations. As they come in as your labor force their approach to technology, security and risk will be different. This generation doesn't necessarily view IT as a risk element."

Participants agreed that simply banning new technologies from the workplace would not work because employees would either break the rules or not come and work for a company in the first place. As Bobbie Stempfley from DISA put it in the context of the military: "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 panelists also noted that the tables could be turned—companies are now also using Facebook and other sites to get information about job applicants.

Some panelists also noted that even more traditional (older) users are starting to adopt the new generation of technologies, and that businesses need to recognize these changes and build their processes and rules accordingly. Goldman's Venables called this process "application disintermediation". He noted some emerging situations where users, instead of requesting application functionality, will request direct access to data to permit their own local innovation, using office productivity and communication and collaboration tools. Unless managed carefully this represents data leakage risk, as more information is flowing around environments which, by default, are more open than the business would like. This drives deployment of tools like digital rights management and more fine-grained access controls so that the business can support this type of innovation without placing information at risk.

The group agreed that it would be a losing battle to simply ban the use of emerging communications tools and applications. A more realistic approach is to manage their use, while educating employees and users about the risks associated with these technologies, and holding them accountable if they break the rules.

In some cases, it is regulation holding up the utilization of new technologies. The legal and regulatory environment that companies find themselves in can be slow to adapt to changes. For example, one participant explained that certain restrictive policies that his firm has concerning electronic communications are not due to company-internal worries about security risks introduced through the use of those technologies, but due to regulatory pressures. Difficulties that have been encountered in this context include having to shut down internal blogs because they were treated in the same way as more official forms of communication. The rise of eDiscovery requirements in general is forcing companies to re-evaluate their tolerance to the use of new technologies.

Changing the Information Risk Mindset

Continuing in a moderated roundtable format, participants discussed the biggest challenges to helping their organizations manage risk. A poll of the group showed that many still have a long way to go. The participants were asked, on a scale of 1-10, where do they think their firm is, with:

- 1 being the CISO should simply make us secure and call us when it is done.
- 10 being everyone is involved in information risk decisions, making economic and risk trade-offs, and information risk is part of every business discussion.

The results (see Exhibit) showed that half of the executives gave their firm a 5 or lower, and none of the firms rate themselves higher than an 8.

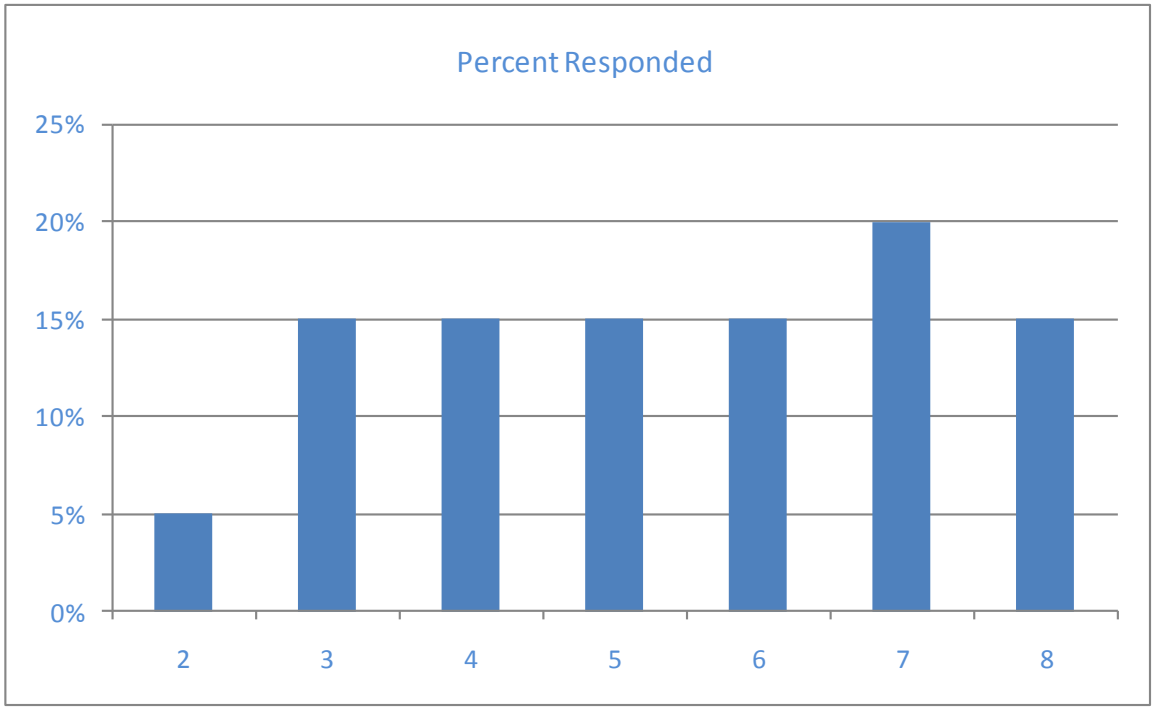

Exhibit: Ranking of information risk awareness and participation within firms.

With these results before them, the group focused on how risk is perceived within organizations; examining the role senior executives play in information risk; attacking the biggest security challenges, analyzing changes in the nature of risks; and managing information risk in the context of partners and supply chains.

Developing risk-based priorities. One of the central themes of the workshop was trying to understand the best ways to prioritize security actions and investments based on the risks a company faces. This move toward security as part of overall risk management was a pervasive goal among participants. Increasingly, security issues are being discussed by companies alongside other risk factors, although they often still don't receive equal emphasis from senior management. Robert Nowill from BT explained the situation as follows: "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."

Another problem in this context is that security risks still seem somehow exciting and mysterious—an image that security executives initially cultivated in order to get senior management's attention and open their pocket books—and are, therefore, not addressed in the same way as other business risks. As security moves more into the mainstream of risk management, the security conversation has to move away from a focus on "black magic" and toward the duller language of business control. Venables explained how the new focus on security as a business control problem has been very productive: "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." However, the extent to which security is becoming part of a company's overall risk management process also strongly depends on the type of organization and the industry involved. Some firms are further along this process because they are in heavily regulated industries where security has invariably become a senior management concern.

One of the major challenges that participants identified was getting senior management to really understand why security is essential. Some companies already 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 it doesn't get in the way of delivering products and services as fast as possible or, more importantly, as fast as their competitors. The focus on the notion of business agility means that security is still frequently viewed as an impediment, which makes the case for better security harder to articulate. As cyber threats grow and the potential consequences of cyber events increase, senior management needs to understand that security is truly a first order risk management issue. "Our direction from the top is to avoid death by a thousand scratches, i.e., implementing thread-based security and control precautions one regulatory/third party requirement at a time," said Russ Pierce from CVS Caremark. "To this end, we embrace industry standard frameworks and best practices for evaluating and securing the organization. … Bottom line, management wants to make the appropriate investment so they can focus in other areas without having to constantly look over their shoulder every time a new industry security/control problem rears its ugly head." There was also a fear that security enlightenment would only come on the heels of having suffered a damaging incident. As IBM's Linda 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?'"

Participants also wanted to get away from the mindset of having to eliminate security risks entirely. In the past, the security group has served as a security blanket: senior executives expected the CISO to reassure them that they were safe against viruses and hackers. However, it is more realistic to acknowledge that perfect security is unattainable and that the goal should be risk mitigation and not risk elimination. Such a risk mitigation approach is much easier if it is couched in the framework of risk management, where the trade-offs between risk and return are already familiar. Jeff Sherwood from H&R Block summarized the point: "What I feel that people don't get is that risk needs to be communicated holistically. Our job here is not risk elimination; it's risk mitigation. There's always going to be risk. If you wake up in the morning, there's going to be risk. 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."

Measuring security. At the last CISO workshop, about 18 months ago, security metrics were high on the executives' agenda. This time around, participants said they were using numerous security metrics in their organizations to measure all sorts of technical inputs, such an the number of attacks a company is facing, the number of hits it gets on its firewall, the number of privacy breaches it has, the percentage of documents or messages it encrypts, or the number of people that receive security training. However, while

the use of metrics has matured and remains important, their shortcomings are also becoming more apparent. DISA's Bobbie Stempfley explained how measuring security was actually having a negative impact at the defense department in terms of limiting 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 in helping to combat the current generation of threats, but are inadequate in helping a company deal with new challenges. As IBM's Linda Betz put it, "We have measurements. We break it up by geography. We break it up by business units. There are report cards. People know where they stand and it is a career-limiting move to not be green on the report cards, whatever green ends up being. 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?"

Education is key. Security leaders continue to emphasize the important role that education at all levels of the organization plays in improving security. Since almost everybody within an organization deals with technology or data, they all need to understand how they could represent a point of vulnerability, and what they can do to help protect the company. Russ Pierce explained that at CVS, "Awareness, especially role-based awareness, is a significant component of our overall strategy; we recognize that in order to achieve, and maintain, good security we need to empower all employees with the appropriate knowledge to work securely with today's, and tomorrow's, technology."

As security education is seen as an important element of a good security program, participants were thinking about making further improvements to their education initiatives. For instance, one company does annual security courses for its 330,000 employees, keeps track of who has taken security training, and security and privacy information is included in business guidelines. However, such a large program is in danger of reverting back to the check box mentality, so efforts are underway to customize training to different kinds of users with different exposure to technologies. Venables said that Goldman Sachs has developed a novel form of education that includes an assembly of people in controls role and beyond that comprise an "incident learning network" that regularly reviews internal and external events for learning opportunities. The external events are probably the most interesting as it gives an opportunity to learn from the mistakes of others before it may happen to you.

Financial or other incentives were also discussed as aides to a successful security education program. While sticks are still widely used, the focus of the discussion was more on the use of carrots. However, only a handful of the companies represented reward employees with financial incentives for good security behavior. While some firms use money to incentivize good security, others offer gifts, such as wine, event tickets or consumer electronics. Eaton has an eStars program, whereby employees can earn eStars for certain actions; these eStars can then be turned into various gifts. Incentives can be doubly impactful because they not only make the recipients happy, but also send a symbolic message to the organization that good behavior will be rewarded and bad behavior will be punished. Terri Curran explained how this works at Bose: "We give product. For us, product is a very big incentive because we make very expensive products and many of our own employees can't afford to buy them. So for us to give away our products is real sign of stature in our company."

Aligning security with a company's culture. Another point of widespread agreement was that a firm's security program has to be aligned with and embedded in its corporate culture. Swimming against the current of the company's culture will not yield success because there won't be organizational support for the security program. For example, Bill Gabby explained that Cargill is a formerly family run, privately held firm. 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. Firms that are heavily regulated and

need to abide by HIPAA or the Sarbanes Oxley Act have an advantage because they have a clear security driver that is important to senior management.

One way to better align security with the corporate culture is to explain how security helps to protect the future of the firm, or as Lee Warren from United Technologies put it: "You have to make sure that your security approach matches your corporate culture. 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 a way to proactively embed security into the company's culture by piggy-backing on other corporate functions: "It has become clearer to me that information risk is multi-dimensional. Therefore, I think it's important to 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."

Protecting intellectual property. As many participants viewed risk to intellectual property as one of their greatest challenges, it was not surprising that the protection of IP is a priority for security executives. 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?" Gabby from Cargill 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 also play an important role in the fight to protect IP. 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.

Several participants considered whether the battle to protect IP can even be won, and companies should instead focus on out-executing their competitors, or prioritizing the protection of only very specific bits of IP. Because IP is so much easier to steal in the digital age, and so many products can be rapidly reverse engineered, new approaches may be necessary. As 3M's Brenberg put it, "We're aware that everybody can reverse engineer. 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." IBM also prioritizes the IP that is the "keys to the kingdom". Added controls are put in place to protect the most important IP, not to protect it indefinitely, but to give the company a six month head start on its competitors. Venables explained that 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.

Securing the extended enterprise and partner relationships. In a global economy, firms increasingly have deep and wide extended enterprises, supply chains and partnerships that are crucial to the success of the business. The continuing trend toward outsourcing and offshoring to places like India and China increases a company's potential risk factors. Even if a company's in-house security program is strong these 'external' relationships put the company's data and IP at risk because security standards at partner

organizations may be weak. As General Dynamics' 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."

One of the problems is that many large companies interact with hundreds or even thousands or small businesses, many of which simply don't have the resources or expertise to implement strong security. Nonetheless, these small businesses may hold important data or IP. As Cody explained, Aetna has been examining all 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 noted that they had started offering 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 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 approach companies are starting to explore to reduce risk is to try and consolidate the number of partners they are doing business with. Raising the level of security at all partner firms may be difficult, so re-evaluating the number of partnerships that are necessary and ensuring that remaining partners meet minimum security standards seems to be a promising strategy. Debra Cody described Aetna's recent approach to partnerships: "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, in order to force economically motivated decisions. This has resulted in more rational outsourcing growth.

A big part of the risk equation when it comes to partnerships and extended enterprises derives from legal and cultural differences across the globe. This means that companies can't "use the same looking glass" for the different places they are active in. Cargill's Gabby put it, "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, different legal environments around the world are an important risk element. In some countries IP laws are non-existent or poorly enforced, 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." Understanding these cultural and legal differences and developing security measures to embrace them will help companies better protect their data and IP.

Security Transformation

In a series of three breakouts, participants pushed deeper to understand effective methods of ranking, communicating, and measuring risk. The goal was to go beyond understanding best practice to developing an action plan to move forward in the next 12-18 months.

Ranking the information threats. The breakout groups looked at questions like: 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?

One of the main realizations was that information risk management is increasingly being integrated into the broader enterprise risk management conversation. However, this development is uneven—there are still some firms where information risk management is focused more at the project management level. Neil Hershfield gave a good summary of the real objectives of Dow's risk prioritization activities: "In terms of prioritizing the threats, two things came to mind when I first heard you ask the question: No. 1, we've got to secure our sites, our chemical sites. So the process of keeping control of our systems and not letting somebody hack in is a big deal for us because if somebody does that, they could cause an incident. The biggest threat is some kind of actual physical incident that's created through cyber. Second, I would say is just in terms of everything we read and see is the risk of insider problems."

One thing was clear. Risk management is structured in different ways at different companies (i.e., there is no single, unified methodology that is widely used to identify and prioritize risks). In some cases risk management is based around applications, in other cases the focus is on assets or specific projects. In some firms, the emphasis is on aligning information risk management as directly as possible with business strategies.

Participants shared with the group how they prioritize and rank threats. It soon became clear that there are lots of different approaches to risk management and ranking risks along a spectrum from the more quantifiable methods (we measure this) to the softer (we know through experience or through interviews) and intuitive (we just kind of know) methods.

There was a lot of common ground in terms of the elements that firms use to help them categorize and address risk. Common risk elements included data classification; governance; compliance; brand; insider risk; infrastructure; availability; and mission assurance. Different firms use a different combination of these elements to structure their information risk management programs; they also weigh the elements in different ways. Underneath each of these high-level categories, firms have a second-tier of specific factors (often data-driven) that they use for their risk evaluations and prioritizations. The risk elements are then viewed in the context of other company-specific factors, such as the state of current control (i.e., the security baseline); the sophistication of vulnerabilities and threats; the cost of mitigation; the potential consequences of inaction; and, in some cases, the infosec impedence (i.e., the risk to program execution or the risk to innovation if information security controls are put in place). The notion of impedence is particularly novel. Once in a while, a company should step back and make sure that protective measures that once made sense are still necessary and are not still in place just by default. Such an approach may help realize additional business opportunities or justify security spending.

United Technologies is using structured approach for overall risk management calculations. Elements of the model come from all business functions. Some of the elements that help feed the model include data classification, governance, insider risk and infrastructure. As Lee Warren explained it, "We're just starting down this path. There's a lot to do. What we're doing is we pick the risk and we take what we think of as large risk areas and we plot them on an eMap. For instance, governance, how are we doing on governance? Are we red, yellow, or green? And then what we do is that we try to make a more

mathematical model by digging down deeper into why we think governance is in the green. And then we'd weigh all those attributes. And then in future years, we'll add to it as the environment changes. If some of those attributes change, then we'll automatically shift those as opposed to being subjective. But the point is, we're trying to put a structure around the whole thing, starting on a very high level."

Several companies are using some version of a risk matrix that has the X axis dedicated to the potential 'Impact' and the Y axis dedicated to 'Probability' of a negative outcome. Different elements of their risk management approach are plotted on the matrix to see how much attention they require. A potentially high-impact event with a high probability of occurring would require an immediate, focused response. These matrices are updated regularly, perhaps quarterly, to reflect changes in business priorities and the risk environment. BT uses a process called BRAT, which is a step-by-step, ladder process where each hurdle has to be taken in order to move to the next step in the process or project. Some of the steps that would need to be overcome could include: Is this legal? Is it in line with contractual obligations? Does it adhere to established business processes? Is there sufficient protection of sensitive data?

An interesting outcome of the discussion was that it became clear that several companies use back testing (i.e., applying actual incidents or audit and assessment findings) to validate or calibrate their risk management approaches and methods. This focus on continuous improvement seems promising in an area that is still immature.

Various companies are starting to use tools to help them identify and rank their risks. Some of the tools include Archer Technologies, RiskWatch, and SecureCompass. John Stewart explained how Cisco is using the RiskWatch tool to help prioritize its risks: "The software itself is an application. The input is by an individual. For example, let's say you would want to take a set of government audit requirements against your environment, and it's a formal set. You put them in, and then are entering them in the known state as you can ascribe it today as any audit would traditionally do. That's subjective data. Then you take the objective data, which is what the audit findings are, of any of your given facilities by the external auditors, and then, over time, it will assert what the categories of risk are with an objective equal to your current areas of effort sorted ostensibly by priority. That's the thinking. Now the question is how people will actually use it. We're going in with the idea that that becomes our risk methodology, so our risk process is subjective/objective data in; this is then sorted and ordered into a priority list of areas to work on. The input doesn't have to be just one project. You could put many projects in, or you could put a business process into it." Others are using similar tools to help them with data classification, security awareness and making the risk prioritization process more objective and repeatable.

There is no single, established process or method that is universally used for ranking risks, but information risk management is maturing and becoming more integrated with overall risk management programs. The use of tools to help rank and prioritize information risks is also becoming more common.

Communicating the information threats. The group examined the following: 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?

Participants emphasized the importance of storytelling in getting the security message across. Telling a compelling story—both in terms of scenarios and using external events to tell a story about how something happened—can be a powerful methodology. Through a good story people can better visualize a problem or risk and find it easier to understand the implications of a potential security event. However, participants stressed the importance of having the story be accompanied by some analysis that makes the story relevant for a particular company. Sheldon Ort from Eli Lilly emphasized that, "It's the limits of imagination that preclude us from taking seriously some of the real risks out there. It's going to that next

step to try and bring it in to a realistic scenario that they can relate to." So, for instance, some threats make great stories, but a firm may already have security measures in place to defend against them, while other stories can really highlight a company's specific vulnerabilities. Security-related stories will be most effective if they are told in the context of a firm's risk environment and goals.

Tuck's Eric Johnson explained, the psychology of risk provides many important lessons for security communications. Story telling is linked to several important concepts of risk psychology including: availability (how readily a personal can recall and idea), limits of imagination (the believability of a concept), or vividness (specific details that support an idea) each have important impact on risk attitudes and actions. For example people systematically underestimate risks they can't imagine. If you can't tell a story about something, or if you can't imagine it, then you're going to assess a very low risk to it or very low probability of its occurrence. The lesson for security communications is that if you can make someone imagine something, they will assess the likelihood of that event actually taking place differently. Much risk communications tend to be boring and lifeless. However, if security risks can be made more real and vivid, people will take them more seriously and assess them as more important.

The group also talked about the strong need to have awareness of the audience and how important it is to interface at different levels, to really know at different levels what it is that the audience will respond to. The point was not that a story should be changed for different audiences, but that it should be packaged and emphasized differently—"hitting the right notes for the right level of audience", as one participant put it. Further, the importance of creating a dialogue and engendering real engagement, as opposed to just doing a briefing, was also highlighted by the group. Mauricio Guerra from Dow related how up until recently they had always just gone into the board every six months and told their half-hour story, their PowerPoint, and left with a "Thank you very much," and how important it was that they've recently changed to a much more dialogue-oriented discussion where the board is actually engaged and suddenly the board cares much more about security risks.

The timing of security communications is also an important factor. Sometimes it is possible to get senior management's attention if a message is communicated on the heels of a high-profile event or new regulations. In the words of Pete Stang from General Dynamics, "But this interest is perishable, whether it's 9/11 or SOX. You have their attention and the board will listen to you for a short time. But after a while, they get bored with it and they'll move on to something else, or they get annoyed with it. We found that out. So you've got to jump when you have the opportunity because you'll lose that window."

Another method that was suggested to help informally spread the security message was through the rotation of people. In some firms security people are sent out to spend a day, several days, or even several weeks in the company's operational units - in the factory or a store or a distribution center—in order to get a better sense for the real operational needs of the business. Cisco has taken this approach one step further, sending some of their best security people to work permanently in different jobs elsewhere in the business. That's one way to inculcate security within the company. Several participants spoke about their goal to make more use of informal communications across different levels of their organizations in order to improve their security posture, and increase awareness of security risks.

Another communications strategy was hitching security communications to other successful wagons in a company. For example, if a company pays a lot of attention to their audit group, legal, or regulatory compliance, then it would be a productive approach to partner with those groups to raise awareness about security. This works especially well with groups where there's already a natural affinity that can be echoed. In other cases, piggy-backing security on successful or topical initiatives, such as privacy, within a company can also bear fruit. Terri Curran noted that she successfully worked with R&D at Bose to help communicate IP risk. Working with R&D was naturally helped move the security agenda forward because, at Curran noted, "In our company, R&D is the driver. It's the lifeblood of what we do."

While many participants had extensive and sometimes innovative internal communications programs, a clear need was identified to ramp up security communications with supplier and partners all the way up and down the value chain.

Measuring progress. The breakout groups examined the following issues: 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?

Measuring risk, or security metrics, had been a central theme at the last CISO workshop. While it remained important, it was becoming a more practical piece of any good security program.

One of the key questions remains what are the things that should be measured. Most companies now have a variety of security measurements that include empirical or systems data such as the number of hits to the firewall, the number of viruses detected, the percentage of machines patched, the percentage of communications encrypted, etc. Specific programs, such as awareness and communications, are also measured, for instance, by capturing how many people have gone through training. Standards or regulations are also used to measure a company's posture against.

Many companies have dashboards and displays that are fed by the measurements to show the security status of various functions. For example, they could be red, yellow or green on fighting spam, based on some internal metrics. However, a big concern that was repeatedly expressed was that measuring security was becoming an exercise in checking boxes, which would not necessarily make the company more secure or better able to handle new risks. The dangers of such a check box mentality include complacency and a loss of personal initiative and innovative thinking. Therefore, participants have spent a lot of time thinking about what other elements they want to be able to measure. For example, how do you measure behavioral change or the management of risk over time? Such measurements have to incorporate certain intangibles, including future forecasts.

Ideas concerning how to measure security were also discussed. Companies use a variety of different techniques and methods to measure security, including information from self assessments, audits, objective risk scoring, compliance efforts and interviews. In some cases, context can be added to empirical rankings through the use of scenario stories. There are also many ways to display and structure the results of measurement. The use of rankings and dashboards is still very common, but other options, such as heat maps and maturity models, are also being explored to express risk effectively.

Measuring risk still remains problematic for a number of reasons. One of the main difficulties is that the risk equation requires some level of quantification of the threat and the probability of that threat occurring. These two elements are notoriously hard to quantify, thereby making some of the other risk metrics less effective. Another challenge is measuring progress—is my company improving its security posture? The threat landscape and a company's vulnerabilities and technologies change constantly, leaving few options in terms of measuring continuity. Good security measurements have to be able to adapt to internal and external changes. Finally, how are security metrics used, and how much faith is placed in them when it comes to making business decisions, including investment decisions? These are questions that need to be explored further.

Looking Forward - Preparing the Organization to Protect Itself

Based on the outcome of the breakout sessions and other discussions throughout the day, the group identified and discussed key lessons for building information risk into an organization's DNA. Among the

topics covered were reducing the risk of information leakage; risk reduction through better privileging and provisioning processes; and defining "security at the source".

Information or data leakage has become a pervasive problem that keeps making headlines. Much of this leakage can be ascribed to the actions of individual employees or partners. Participants discussed best practices and solutions from their organizations that are being used to reduce individual data leaks. These solutions are both technical and non-technical.

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 has to be followed by a clear policy surrounding data protection, with clear rules on who has to protect what. Moreover, the policy must be crafted in such a way that everyone feels personal accountability for protecting data, and it must be enforced in order to be effective. Nancy 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 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 emphasized data classification and subsequent protection policies are not awareness tools, but are there to hold employees accountable. As one 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."

About half the participants said they were using some kind of content monitoring tool to help protect their information against leaks. The most popular tools that were cited were Vontu, Tablus, Vericept and Orchestria. The main reason that tools are being used is that data is so hard to keep track of and much of the leakage that occurs is accidental. Tools can help a company get their arms around this massive problem. 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. Said CVS's Russ Pierce, "Given the volume of information flowing in and out of an organization you could easily get overwhelmed with these products. To be successful, it's imperative that you pick your battles based on information classification or type. It's 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 Jeff Sherwood called the "friendly fire of information security", that need to be investigated and followed up on. Several firms have implemented an automated response to data leakage that is identified by their monitoring tools. This can take the form of a warning message to the employee that is suspected of leaking the information, or the message could simply be blocked.

Another important element in protecting a company's valuable information and data is effective provisioning (i.e., providing people with the 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 taking away access to information and resources when people leave the company or no longer need to use that resource. A number of attendees already have processes in place for provisioning. In the case of IBM,

some of these processes are long-standing, as Linda 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 Debra Cody agreed that provisioning can be very useful, especially if it was 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. 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 recertifications that we have automated through the workflow for our Sarbanes Oxley compliance."

In the end, 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 and those issues will only be solved by building information risk practices into the organization.

Panelists, Participants, and Research Team
Security through Information Risk Management
October 5, 2007

Rodney Baker	Head of Infrastructure, Region Americas Adidas Group
Susan Bates	Vice President and Manager, Information Systems Security and Compliance Solutions BJ's Wholesale Club
Linda Betz	Director, IT Policy and Information Security IBM Corporation
Hans Brechbühl	Executive Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
John Brenberg	Manager, IT Security & Integrity 3M Information Technology
Debra Cody	Head of Information Security Aetna, Inc.
Terri Curran	Director, Corporate Information Security Services Bose Corporation
Chris Dunning	Director, Information Security Enterprise Information Security Officer Staples Inc.
Scott Dynes	Senior Research Fellow and Project Manager, Center for Digital Strategies Tuck School of Business, Dartmouth College
Mary Erlanger	Director of IT Risk Management, Global Information Technology Colgate-Palmolive
Bill Gabby	Global Information Protection Manager Cargill
Eric Goetz	Assistant Director, Research and Analysis I3P, Dartmouth College

Mauricio Guerra	Global Director of Information Security The Dow Chemical Company
Neil Hershfield	Director, Chemical Sector Cyber Security Program The Dow Chemical Company
Barry Horowitz	Professor of Systems and Information Engineering University of Virginia
M. Eric Johnson	Professor of Operations Management Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
Jack Matejka	Director, IT Security Eaton Corporation
Robert Nowill	Director of Information & Network Security BT Group
Sheldon Ort	Director, Information Asset Management and Architecture Eli Lilly and Company
Charles Palmer	Chair and Director of Research I3P, Dartmouth College
Shari Lawrence Pfleeger	Senior Information Scientist RAND Corporation
Russ Pierce	Chief Security Architect CVS Caremark
Geir Ramleth	Senior Vice President and Chief Information Officer Bechtel Group, Inc.
Jeff Sherwood	Manager, Corporate Information Security H&R Block
Pete Stang	Information Security Officer/Manager of Security General Dynamics
Bobbie Stempfley	Vice Director for Strategic Planning and Information Defense Information Systems Agency

John Stewart	Vice President and Chief Security Officer, Corporate Security Programs Organization Cisco Systems, Inc.
Phil Venables	Managing Director and Chief Information Risk Officer Goldman Sachs
Lee Warren	Chief Information Security Officer United Technologies
Nancy Wilson	Director, Enterprise Information Security Time Warner Cable Corporate