TUCK SCHOOL OF BUSINESS AT DARTMOUTH
Glassmeyer/McNamee
Center for
Digital Strategies
www.tuck.dartmouth.edu/digitalstrategies

I3P
Institute for Information
Infrastructure Protection

Assessing Risk in Turbulent Times

A Workshop for Information Security Executives

Assessing Risk in Turbulent Times[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 examine the new risks and challenges of managing security in a period of economic turbulence. The workshop included security leaders from Adidas, Aetna, Bechtel, Colgate-Palmolive, Dow Chemical, Eastman Chemical Company, Eaton Corporation, Eli Lilly, General Dynamics, Goldman Sachs, Hasbro, IBM, Providence Health & Services, Santa Fe Group, Starwood Hotels & Resorts, Staples, United Technologies and DISA, along with academics from Dartmouth, RAND, and the University of Virginia.

Key Insights Discussed in this Article:

- **The downturn has led to what many see as the perfect storm for information security professionals.** From employee downsizing and stretched budgets to the consumerization of technology and rising professional threats, CISOs are asked to do more with less.

- **Security tools have matured with a steady string of new offerings to address arising risks.** However, the unending stream of new tools can be a distraction from what is, in fact, a human problem.

- **Crown jewel designation can be a helpful way to classify crucial information.** However, it is important to strictly limit such high priority categories or everything, and thus nothing, is a crown jewel.

- **Executive attention on security is a silver lining of the downturn.** As times got tough, boards focused on risk, and information risk bubbled up to the top.

- **Vendor surveys are OK, but thoughtful questions are far more powerful.** While many good assessment surveys are available, CISOs still find that probing questions lead to a dialog that gets to the root of security issues.

- **Third-party risk assessments can be helpful for initial vendor screenings.** But few firms see external assessments replacing internally driven due diligence.

- **There is growing interest in industry-driven assessment methodologies.** But as with third-party assessments, one size doesn't fit all.

- **With new threats appearing at a dizzying pace, developing businesses processes that can operate in an insecure world is the key to risk reduction.** Since anything connected to the internet is vulnerable, simply increasing security is a losing game.

[1] This overview was written by Jeff Moag and Professor M. Eric Johnson of the Tuck School of Business at Dartmouth College. The workshop and research were partially supported by the U.S. Department of Homeland Security under Grant Award Number 2006-CS-001-000001, under the auspices of the Institute for Information Infrastructure Protection (I3P). 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 I3P.

Introduction

The agenda hinted that "Assessing Risk in Turbulent Times," a roundtable for information security executives hosted by the Center for Digital Strategies at Dartmouth's Tuck School of Business, had struck upon a particularly timely subject. Speaking to the workshop participants gathered on Tuck's Hanover, N.H. campus, Chief Information Risk Officer Phil Venables explained Goldman's risk outlook in the context of Peter Sandman's equation: Risk equals hazard plus outrage. "So when we think about the perfect storm, we're thinking not just in terms of hazard, but the outrage factors," he said.

Outrage indeed. Leading the morning roundtable discussion entitled "The Perfect Storm: New Internal Risks," both Venables and Eric Cowperthwaite, CISO of Providence Health and Service, have navigated rough seas. Perfect storm is also an apt analogy for the confluence of risks currently facing information security professionals.

The current threat pattern includes a new generation of tech-savvy employees, nearly universal penetration of information-sharing technologies, and expanding—some would say unrealistic—security expectations. All of these factors are exacerbated by the worst economic recession in more than half a century. The recession means fewer resources at many firms, while layoffs create a pool of highly capable former insiders.

Discussing this rapidly evolving threat environment were 20 information security executives from 17 Fortune 500 firms and the U.S. Department of Defense, as well as several security consultants and academics. Participants represented a broad spectrum of industries, including retail, defense, healthcare, insurance, manufacturing, construction and hospitality. Though many of their specific concerns related to their companies' core businesses, they found much to agree on: the current threat environment is rapidly evolving and increasingly challenging.

"Sometimes even voicing these concerns is kind of frightening, but on the other hand, I think as a group of security executives we can't do anything better than to share information about things we see coming along," said moderator M. Eric Johnson, Director of the Center for Digital Strategies.

The workshop included sessions on evolving internal and external risk, followed by breakouts on assessing risk and a summary discussion of how best to manage it. The session on internal threats centered largely on social science challenges in a contracting knowledge economy.

The Perfect Storm: New Internal Risk

The roundtable opened with the subject on everyone's mind: How do companies control information technology risk when the knowledge economy is in freefall? Workshop participants explored the issues of greatest importance in the current environment: a growing pool of former insiders possessing knowledge, skill and potentially dangerous motives; the ubiquity of social networking; an increasingly crowded and dissonant regulatory environment; the drive for efficiency at the expense of security—all factors that must be considered within the risk-multiplying context of a cratering economy.

Cowperthwaite explained that many of his challenges stemmed from a large professional workforce that expects a great deal of personal freedom. Of Providence's approximately 75,000 workers, about 40,000 are professional employees and 25,000 are physicians, Cowperthwaite said. "Most of the professionals are very well-educated, very well-paid people, and they're used to using smartphones and BlackBerries and computers," he said.

The physicians present an even more daunting management challenge, because they are not employees. "I don't have the same controls over them that I have over those other professionals in terms of employment and sanctions and discipline," Cowperthwaite said. "And they have been taught that they are the ultimate arbiter of what happens in their sphere of influence."

Providence Health maintains personal health and credit information on more than 7 million people. That makes it an enormous target. At the same time it is under extreme economic stress. Healthcare reimbursement rates are shrinking, costs are rising, and Providence's investment portfolio has suffered a body blow. As a result of the poor economy, the organization also is providing more free medical care to the increasing number of people who can't pay.

"Decreasing revenue, increasing charity care makes things look red instead of black," Cowperthwaite said. "That's the perfect storm that hospitals find themselves in right now."

Venables discussed the hazard (of risk equals hazard plus outrage) as a three-sided problem: Highly educated, computer-savvy Generation Y employees, who have access to radical improvements in communication and collaboration technologies, operating in an environment of declining IT budgets. That has resulted in a partial migration of computing functions, and therefore control, from IT departments toward that capable user base.

The outrage also presents as a three-way storm: Magnified reputation risk; potentially unrealistic (but wholly understandable) security expectations from stakeholders (boards, management, or customers) even when they face challenges in adjusting existing business processes to achieve it; and adverse regulatory responses in the wake of negative publicity.

Venables discussed security risks posed by releasing thousands of highly skilled, extremely knowledgeable employees. "Like many financial firms, we downsized some part of our workforce over the past 18 months," he said. "And so we end up balancing the need to demonstrate trust in our workforce and at the same time, monitoring their use of proprietary data."

Scott Lancaster, CISO of Starwood Hotels and Resorts Worldwide, elaborated on the risk of downsizing. "You may find that as you reduce staff, you start combining job functions and, therefore, need to over-privilege individuals. Where you might have had segregation of duties and opportunities previously, you now have one person performing what were previously multiple roles."

The proliferation of startup companies marketing security technologies comes with a disturbing corollary: Anyone who has the ability to build tools to manage information security risk also has the skills to create that risk. So to the perfect storm of cost-cutting and downsizing, Lancaster adds another element. “Highly skilled individuals in various parts of the world, including here in the U.S., who are desperate and want to put those skills to use to generate some revenue stream for themselves, whether it be legal or illegal.”

Into this difficult environment, regulators have continued to add layers of what Cowperthwaite termed “very discrete, disorganized regulations.” While the proliferation of regulations drives cost and complexity; it also has led to a rapid increase in security solutions.

“New tools that we hadn’t even considered just a few years ago exist now, like data loss prevention,” Cowperthwaite said. In January he implemented a $650,000 DLP program, and in July reported to his CFO that the investment already had paid for itself. “So we had about three-quarters of a million dollars in cost avoidance in six months. That is amazing. Nobody ever heard of DLP four or five years ago.”

However Ray Musser, Staff VP for Security at General Dynamics, warned that the unending stream of new security tools can be a distraction. Companies must make a sound business case for these tools, keeping in mind that risk management is ultimately a human-based problem

Human risk has been amplified by the widespread use of social networking sites used in concert with smartphones and other portable devices. One of Providence’s hospitals in southern California frequently treats Hollywood celebrities, Cowperthwaite said. A nurse there used her smartphone to photograph a celebrity and her daughter undergoing treatment in the Emergency Room, and posted the photographs to Facebook. Cowperthwaite only discovered the breach because one of the nurse’s Facebook friends alerted him to it. “Imagine how much computing power I would need to Google Facebook, MySpace, LinkedIn, etcetera, for every possible search term I’d need to search on in order to find out if my employees are doing this,” he said. “I have no way to do this.”

Enabling more flexible, mobile workers also means contending with new risks, noted Don Michniuk, Corporate Manager of Information Security at Bechtel Group. “And the two biggest ones that are on our plate right now are move to cloud computing and move to bring your own computer to work, so our employees will soon be able to bring their own units in.”

A more technologically savvy workforce can be an advantage, noted Sheldon Ort, Manager of IT Risk, Compliance and Process at Eli Lilly and Company. “Our employees are asking the right questions that they never did in the past,” he said. But many are acting without asking first, cautioned Kevin Kilroy, Senior Director of IT Risk Management at Starwood Hotels and Resorts Worldwide. “A little knowledge can be dangerous. They’ll think that they can, for instance, extend our network by simply going up to the local Best Buy and buying a little wireless transmitter. Their attitude is, ‘Well, it has a firewall, so I thought I was just doing the right security thing.’” Employees have to understand the distinction between being a user who is operating securely and being a security practitioner, Kilroy said.

Into this mix comes the question of efficiency and profitability, which thrive best in an environment of innovation and the fluid exchange of information. “The mega-trend that we’re seeing is the expected collaboration both up and down the supply chain,” said Thomas Maurer, Director of the IT Program Office at Eastman Chemical Company. “It’s not just our suppliers. It’s our customers, too. We want to collaborate with them. We want to share information with them. We want them to share information with us.”

While there is sensitivity to security at the executive level, Maurer said there is an expectation that Eastman will collaborate closely with its partners. As Cowperthwaite noted, the dominant business theme of the last decade has been seamless communication and the empowerment of the individual. “Those things are directly contra to information security in general, which doesn’t mean they’re bad things. It just means there’s a reality here that the very dominant theme—not only of business, but of our general culture—is not in line with trying to lock things down,” Cowperthwaite said.

Mary Erlanger, Director of Information Technology Risk at Colgate-Palmolive, noted that efficiency must be part of the message when speaking to the board level. “Anything that relates to increased productivity, reducing costs and increasing innovation and staying competitive and preserving your position and your reputation—those are the things I think we need to speak to when we’re trying to raise the awareness” she said.

Increasingly, CISOs are getting board-level attention. Linda Betz, Director of IT Policy and Information Security Office of the CIO at IBM Corporation, said that she has more money this year for security projects than she had the year before. “We did a really comprehensive job last year on a risk assessment, and we brought it all the way up to the senior vice presidents,” she said. “We were able to describe what our risks were and what we wanted to go invest in. That was able to drive more money to me while almost everybody else was getting cut.”

Evolving External Risks

The roundtable next tackled external risks, touching on a host of emerging and evolving threats. Many of these stem from the changing business environment. The battered economy has resulted in fewer security resources and more personnel risk at some companies. At the same time, a long-term trend toward business efficiencies has increased risk related to joint ventures, offshoring and outsourcing. The roundtable agreed that the attestation process, which many companies use to vet vendors and partners, has some critical weaknesses, principally the usefulness and integrity of the data it yields. On the positive side, participants reported a higher degree of board-level interest in information security, often stemming from breaches within the company or the industry. Aetna for example, is weighing the value of some outsourcing agreements versus the added risk they entail.

Mauricio Guerra, Global Director of Information Security at Dow Chemical, led off the session with an overview of Dow’s business and risk profile. Dow is a worldwide company, with 156 manufacturing sites in 37 countries. The company has roughly 50,000 employees and 20,000 contractors or suppliers, and it operates in critical industries including clean water, agriculture, housing and of course chemicals.

Dow's chief security concerns are twofold: Protecting its manufacturing facilities, specifically its highly automated process control systems; and protecting the intellectual property that is essential to making Dow a globally competitive enterprise. The first has become more difficult as Dow moves away from an old-economy corporate model, in which employees stayed with the company for their entire careers, and toward open-market solutions. The new approach brings additional grief from a security standpoint, as many more people now have knowledge and control of the process control systems. Add to that the fact that many isolated control systems used in production have now been exposed to the Internet as firms integrate and modernize systems and you have "a big, big, big challenge" noted Guerra. Dow, like many firms, also faces emerging challenges with information security related to recent cost-cutting, as well as downsizing and offshoring of data processing functions.

At the same time, Dow is aggressively expanding operations into emerging markets, including India, China, Russia, and Brazil. Much of this expansion comes in the form of joint ventures. In the past, Guerra said, Dow would typically control 90 percent of such businesses. "Now those are more 50/50 type of joint ventures where we need to share our information, but we cannot share all information," for proprietary reasons or because of export controls.

Export controls are not new of course, but in a highly fluid transnational business they become more disruptive and more difficult to adhere to. "When our systems were mainly supported in North America, we were not too concerned from export control. Now if we are supporting that system from China or from India, people from those nationalities cannot be exposed to that information," Guerra said.

Dow adopted a "crown jewels" approach to information security: The company identifies the information that is most critical to the business, segregates it from other data, and guards it more closely. The key, Guerra said, is to be very selective in choosing which information should receive crown jewel-level protection.

Roberta Stempfley, Chief Information Officer at the Defense Information Systems Office, seized on that comment. The Defense Department survives around classification levels, she said. Defense maintains a cryptographically separate network and computing systems to protect its most-secret information. But, Stempfley said, when too much information is given this crown-jewel status, the designation—and the protection—is eroded. "It becomes too commonplace and folks don't appreciate what's really there. So now we have the announcement of the bake sale and all of this happening at that environment. And so nothing is a crown jewel."

Shari Lawrence Pfleeger, Senior Information Scientist at the RAND Corporation and an I3P researcher, related an anecdote from Edward Tenner's "Why Things Bite Back" to the discussion of crown jewels and best practices. In the book, Tenner reports that football injuries are more severe than rugby injuries because football players feel protected by the helmets and pads they wear. "And so I worry sometimes about our best practices because as several of you have mentioned in examples, people say, ‘Oh, there was a firewall, so I thought I could do this.’ They feel protected by the technology when they’re not.”

That false sense of protection comes into play with the attestations and questionnaires many companies use as part of their vetting process. Musser stated the group’s consensus in blunt terms: “We’ve found that some vendors make attestations that aren’t true.”

That has brought board-level attention to the information security process at Aetna, which experienced a highly publicized breach in May. “The process that we’re looking at now involves both business and IT changes,” said Debra Cody, Head of Security Services at Aetna. The company is evaluating from a business perspective the number of outsourced relationships it has, particularly those that involve highly sensitive information. “We’re looking to evaluate whether or not we really need that number [of vendor relationships] or whether we need to bring some businesses processes and systems back in house.”

Board-level interest is one of the silver linings to high-profile data breaches, though everyone would prefer the breach be made by a competitor. That was the case with the Eaton Corporation, where the board’s audit committee asked Allen Mullen’s team for a briefing after it learned of a leak that occurred through one of the subcontractors in the Joint Strike Fighter program. “They were curious about what we are doing to protect ourselves, to make sure we’re not the ones” responsible for the next breach in a highly classified defense program, said Mullen, Eaton’s Manager of IT Security.

Aetna’s Cody stressed the importance of adding contractual teeth to the attestation process, a sentiment that other roundtable participants echoed. *“*One of the things that we try to do quite often, especially when we start on vendors, is to get security stuff nailed down in contracts,” including the right to audit, said Jeffrey Moore, Senior Enterprise Security Manager at the Adidas Group. “Anybody who’s not willing to get audited on our level obviously has something to hide in some of these countries.”

Like Dow and other international manufacturing companies represented in the roundtable, Adidas must share proprietary production processes with third-party vendors, often in parts of the world with little to no intellectual property protection.

The Eaton Corporation is dealing with that question now. Last year the multinational electrical and industrial company made an acquisition that added 8,000 mainland Chinese employees to the company’s network, said Mullen. “It was actually a Taiwanese company and they locked their mainland employees down as tight as a drum.” Meanwhile, the Taiwanese employees had relatively free access to resources on the network and Internet. Eaton is now dealing with the cultural question of whether to continue treating mainland Chinese employees differently than others in the company. “We’re looking at that in not just China, but India, Eastern Europe, Brazil—anyplace where there’s weak or little intellectual properly laws,” Mullen said.

Adidas works to limit counterfeiting of its shoes by producing just one model of shoe in a given factory. In the case of the Adidas 1 “intelligent shoe,” however, the company went a step farther. “They actually compartmentalized all the different sections so nobody had one big picture of how to make that shoe," Moore said. "And it wasn't copied for over a year, which was great. You laugh, but that's really good statistics for anybody."

Operating in multiple countries is always fraught with risk. In some countries—France and China are reputed to be among the worst offenders—the governments actively support industrial espionage. Musser brought up this point with Starwood Hotels' Lancaster. "How do you deal with the host nation that's requesting either access or data from your customers?"

"Very delicately," Lancaster answered. He noted that before the Beijing Olympics last year, the Chinese government instructed Starwood and other hotel chains to buy and install Internet monitoring devices in their hotels. The hotels resisted, and the Chinese eventually backed down, in part because Lancaster got a U.S. Congressman involved. However it would be naïve to think that a hotel can offer absolute protection, particularly in a foreign environment.

"I've had manufacturing companies ask how we would protect information that one of their associates might incidentally or accidentally leave in one of our hotel rooms. My answer is, 'We're not.'"

Any company that relies on a vendor to protect its data does so at its own risk. In this time of evolving threats, it pays to remember that vendors also are also looking for savings, sometimes in ways that compromise security. For example, Musser noted that vendors who off-shore call centers can end up putting sensitive data at risk.

Risk Assessment
Building Internal Capability

Every firm must consider how to build its internal risk assessment capability. Chris Dunning, Director of Information Security, shared the methodology Staples uses to assess risk within eight divisions in 12 countries. Staples has had an option contract in place with a third-party auditor to complete on-site assessments for Staples, but Dunning says that in two years the company has not felt the need to use it.

When assessing risk in one's own company, information security officers can drill down far deeper. At Staples, Dunning embeds his own people within each business division. That makes his job easier—when his team arrives for site visits his embedded team already have the questionnaires completed and interviews scheduled—but also removes cultural hurdles and organizational barriers.

"It seems to be a good practice for larger firms is to embed staff into your business units as part of your risk-management and business-relationship approach," said Providence's Eric Cowperthwaite. "I could have the same number of people in a central organization, but then when they went to visit that business unit, they'd be viewed as auditors, not as folks."

Colgate-Palmolive' Erlanger stressed the importance of the obvious: Just ask. "It sounds really basic, but we forget to do it—ask lots of people at lots of levels what worries them, and then figure out from there what's important." Her colleagues seized on the importance of this mindset, and shared some of their methods for soliciting information.

Eli Lilly is piloting a SharePoint collaboration space to help identify potential threats. "Anyone in the corporation can input a risk, and then we have a risk team to review and consider it," said Lilly's Sheldon Ort.

Lee Warren said he solicits critique of his risk assessments from United Technologies' business units. "We say 'this is how we look at the risk model. Where are we missing?'" Some CISO's will also ask for informal risk assessments from outside the corporation. Lancaster recounted a recent conversation with a risk officer at Cisco Systems, who asks colleagues at Cisco's largest institutional investors how they view the company's risk.

General Dynamics asks inside the company and defense industry peers to assess potential weaknesses, but doesn't stop there. "We use both internal and external consultants to actually do risk assessments and attacks against applications," Musser said. "We have a robust audit process that is given senior-level attention including board reporting."

That level of attention reflects the importance of security within the defense contracting business, where stakes are high and threats include everything from garden-variety hackers to state-sponsored espionage. "The loss of a single algorithm could potentially render a contract virtually worthless," Musser said.

However deep a company's risk investigation goes, it begins with a questionnaire, and the design of that process will typically set the tone for the deeper analysis. Dunning explained the Staples process, which for any external business relationship begins with six prequalification questions. "From these questions we determine, 'Yeah, they have their act together,' or, 'Oh, no we need to sit down and talk to these guys,'" said Dunning. One of the prequalification questions is whether the vendor has an established corporate security policy and standards in place. One vendor recently answered, "No, we don't. Can't you give us a policy that you use?"

The Staples internal protocol uses a set of 90 questions—five detailed questions in each of 18 areas. These questions are backed up with on-site interviews of 15 to 25 people in each business unit, depending upon the size of the organization and the distribution of duties within that division, Dunning said. This is a somewhat lighter questionnaire than the 200-question CIS survey, and it is dwarfed by the more than 1,600 questions in the full-fledged BITS SIG that Bob Jones described in the breakout on cooperative risk assessment. Those questionnaires are designed to assess a much broader array of business functions and practices; Staples questions can be more directed because the areas of business they are designed to assess are more defined.

Participants agreed that a color-coded or numerical score is desirable, particularly when dealing with vendors and internal business units, or reporting to the board-level. However, as Hans Brechbühl, Tuck's Center for Digital Strategies Executive Director, noted, risk scoring alone is not a substitute for a more comprehensive understanding that comes from deep familiarity with the assessment tools and, more importantly, a gut-level understanding gleaned from interviews and on-site visits.

"I don't think [risk assessment] can be reduced to a questionnaire. There are too many questions or not enough questions, and you don't know the right questions to ask," said Erlanger. "I really think it has to be a dialogue that you have that depends on the service that you're getting and what the expectations are." That points to the essence of risk assessment: Some see it as a science, others more of an art. The prudent approach therefore combines metrics with rigorous on-the-ground due diligence.

Risk Assessment Services

John Nye, a former Assistant Vice President at Moody's Risk Services, described that company's Vendor Information Risk Rating assessment methodology. Moody's began the project at the behest of several Wall Street firms, but market factors forced them to withdraw. The bulk of the discussion focused on the economic viability of such a service: Is there sufficient demand? How much would companies be willing to pay for this service? Could the audits meet the specific requirements of each company? And which of the parties would be liable in the event of a critical data breach? As Robert Hutzley, Manager of the Information Security Organization at Hasbro, said: "Who owns the risk?"

While there was widespread agreement that a risk-assessment rating similar to bond- or credit-rating services would be a useful tool, participants were uncertain of how firms would use results. The market for third-party risk assessment would likely be as an adjunct to internally run audits, as a more cost-effective way to show regulatory compliance in low-risk areas of their business, or as a filter to exclude unsuitable vendors before undertaking more rigorous in-house due diligence.

To be economically viable, a risk-assessment service would have to sell each audit it conducts multiple times, Nye said. At the same time, it is difficult to create one audit that meets the unique needs of every customer. Lancaster described the problem: "What's important to me? What is our relationship with that vendor? What is our technology environment? Because, quite frankly, unless you really understand all of that, the assessment is going to be so high-level and generic that it's not really going to be very useful."

Some companies that have considered custom third-party audits have found that they could do the work internally for less. Kevin Kilroy, Senior Director of IT Risk Management at Starwood, brought up the example of a relationship his company was exploring with a European firm. "We were doing the type of business where it behooved us to do some in-person discussions, and the question was: How much would it cost us to fly over there and conduct that, versus someone from one of the big consulting firms? The answer was that it is cheaper for us to do it ourselves, and, frankly, it probably would be more thorough."

The level of comfort with third-party audits is closely related to the risk inherent in the business relationship. While a generic third-party audit might be sufficient to vet a coffee supplier, none of the practitioners present would rely exclusively on an outside service to assess a vendor that would have access to the crown jewels. The question becomes more nuanced in the middle range of the risk-exposure scale, which is where a third-party risk assessment service would either succeed or fail. Having an off-the-shelf solution to regulatory requirements is an attractive option. That's what the financial firms that approached Moody's to develop a vendor risk rating product were looking for. "What they needed was a scalable solution so they could meet a regulatory requirement and then do the best-practice security work in risk management around that," Nye said. Moody's based its methodology on those of the Wall Street firms on its advisory council. The result, Nye said, looked a lot like the ISO 27002 information security standard.

The Moody's product rated each service provided by vendors separately, rather than entire companies. That allowed for a more modular analysis that was more likely to be valuable to the specific customers of each rated service. These more generic reports could be a valuable piece of the vetting process that also includes internal due diligence. "In a financial scenario, just because somebody's Double-A bond rated doesn't mean you don't go and in and do some due diligence," said Providence's Eric Cowperthwaite. "But you might be able to remove some of the uncertainty."

One of the problems that any auditor faces is that people invariably put their best face forward when they know that their practices are under scrutiny. Discovering potential vulnerabilities often takes some detective work, whether that means making a few discrete phone calls to colleagues at other companies, monitoring peer-to-peer reporting Web sites like www.yelp.com, or taking references out for a nice dinner. "Wine really does bring out the truth," said Adidas' Moore. "And Germany has some really great beer."

Industry Initiatives for Shared Assessment

A straw poll of workshop participants showed that the desirability of shared assessments varies widely by industry, but has not been universally accepted in any sector. Just as they did during the breakout discussion on third-party risk assessment services, information security executives said they were wary of ceding ultimate control of their company's risk assessment process to a third party. However, participants saw value in such programs as filters or adjuncts to their endemic security protocols.

BITS introduced its shared-assessment program for the banking industry in 2006, and the program has gained a measure of acceptance in that sector, said Robert Jones, a Senior Consultant with the Santa Fe Group who works with the BITS program. Cooperative risk assessment efforts have also gained some traction in healthcare, with the advent of the HITRUST Common Security Framework, a pay-to-play program touted as a one-stop data security solution for the healthcare industry. The defense industry has some ad hoc mechanisms in place to share information about threats and breaches. Existing government resources also include the Treasury Department's database of criminal breaches.

The BITS program is based on an in-depth Standardized Information Gathering (SIG) questionnaire containing more than 1,600 questions. Vendors complete the SIG on their own and make it available to potential business partners. Vendors may also hire security or accounting firms to perform an independent on-site assessment using a protocol that BITS supplies.

Vendors realize cost savings because they only have to respond to the BITS SIG, rather than answering a proprietary SIG for every potential business relationship. That creates efficiencies at both ends of the relationship, Jones said.

BITS does not score the data or rate vendors; the financial institutions analyze the data and determine whether a given vendor represents an acceptable risk. The institution can either accept the self-assessment, go back to the vendor and ask for an independent on-site assessment, or conduct an on-site assessment of its own.

Charles Palmer, Director of Research at the I3P, drew an analogy to web sites like Angie's List. "If I understand your proposal," he told Jones, "I would use this like I use some of the local web sites where you could post things about plumbers in the area. I might eliminate some people that way, but it would be a very rare case that I'd use it for a final decision."

One drawback to this approach is that any questionnaire capable of satisfying a large number of end users quickly becomes unwieldy. "If you have something that large, then it is incumbent on somebody to customize it for the particular situation," said Mary Erlanger of Colgate-Palmolive. "And then it isn't standard any more, right?"

BITS addresses that problem by using a tiered SIG. While the full document weighs in at more than 1,600 questions, a 57-question version called SIG Light has been developed, Jones said. "Question number one is 'Do you have information security programs?' If the answer is no, well, then you don't have to answer any other questions."

Citing the "gray areas" in PCI questionnaires, Lancaster said the information such forms provide isn't precise enough for his purposes. "I couldn't put any value in the integrity of that data, not because I worried that the third party might not be honest, but because there's so many varying interpretations of those questions that a yes or no answer—or even a one-sentence explanation—isn't really going to tell me enough about the risk I am assuming."

Lancaster is no fan of questionnaires. In his seven years at Starwood, he hasn't completed a single one. His legal department won't let him. "I'll get on the phone for hours, as long as they want, and talk about what we do, how our program works. We will not document that in writing, though. Anything I put in writing would be a point-in-time evaluation." That these evaluations have limited shelf life calls into question the core assumptions underlying the shared-assessment concept: That if someone else already has performed an assessment, there's no need to do one of your own.

Despite such reservations, the BITS model is gaining measured acceptance in the financial services industry. Document backup service Iron Mountain relies heavily on the program. HITRUST has made similar inroads in the health sector. Most of the industries represented in the workshop expressed some degree of interest in cooperative assessment as one piece of a larger information security protocol.

Managing and Reducing Risk

Moderator Eric Johnson framed the concluding session on managing risk with a question: Imagine a world with no security. Given that the ‘new normal’ is more volatility, can we build business processes that can operate without security? Ann Halford, Vice President of Worldwide Security at Staples, answered with the provocative notion that we already are living in that world. When two people are responsible for monitoring 200 million credit card transactions a day, she said, “What happens when someone is sick?”

Staples’ response has been to lock up the crown jewels and limit outside connectivity as much as possible. Halford reduced the number of in-store applications from 32 to 14, and introduced the use of tokens in lieu of credit card numbers. By using tokens or truncating sensitive information, many business processes can operate without the need for ironclad security. Other roundtable participants endorsed that approach. A risk-based approach should be used because it is virtually impossible to protect everything in a company network.

Of course, no one around the table wanted to unilaterally move to a world without security. As Starwood’s Scott Lancaster noted, some “prominent people in our industry are saying we don’t need firewalls and anti-virus software. The CIO goes and talks to them, and when he comes back he raises cost issues (of maintaining those controls).” While many agreed with the point that firewalls, by themselves, don’t equal security, few CISOs were ready to pull the plug.

Phil Venables’ introductory comments to the group still hung on everyone’s mind. At earlier roundtables, much discussion had focused on resilience—the notion that we assume bad things will happen and that we design business processes to be fundamentally resilient as opposed to just having some form of backup/recovery (i.e. if you take out one node of the business it should carry on running). But to push the idea further to a more fundamental and challenging problem: Can we design business processes that could operate effectively in an environment where there is no security whatsoever? In other words, how would one design a survivable and effective business without being able to call upon controls to mitigate risks while being exposed to endless threats? The Roundtable adjourned to Murphy’s Pub to debate that one.

Participants and Research Team

Assessing Risk in Turbulent Times
July 14, 2009

Linda Betz	Director IT Policy and Information Security Office of the CIO IBM Corporation
Hans Brechbühl	Executive Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
Debra Cody	Head of Security Services Aetna Inc.
Eric Cowperthwaite	System Director & CISO Providence Health & Services
Kenneth Crowther	Research Assistant Professor University of Virginia Center for Risk Management of Engineering Systems
Chris Dunning	Director, Information Security Enterprise Information Security Officer Staples, Inc.
Scott Dynes	Senior Research Fellow Center for Digital Strategies Tuck School of Business, Dartmouth College
Mary Erlanger	Director, Information Technology Risk Management Colgate-Palmolive Company
Mauricio Guerra	Global Director of Information Security The Dow Chemical Company
Ann Halford	VP for Worldwide Security & Enterprise Architecture Staples
Robert Hutzley	Manager of the Information Security Organization Hasbro
M. Eric Johnson	Benjamin Ames Kimball Professor of the Science of Administration Director, Center for Digital Strategies Tuck School of Business, Dartmouth College

Robert W. Jones	Senior Consultant The Santa Fe Group
Kevin Kilroy	Sr. Director of IT Risk Management Starwood Hotels & Resorts Worldwide
Scott Lancaster	CISO Starwood Hotels & Resorts Worldwide
Thomas Maurer	Director, IT Program Office Eastman Chemical Company
Don Michniuk	Corporate Manager of Information Security Bechtel Group
Jeffrey Moore	Sr. Enterprise Security Manager Adidas Group
Allen Mullen	Manager IT Security Eaton Corporation
Ray Musser	Staff VP - Security General Dynamics Corporation
John Nye	Information Risk Management Consultant Independent
Sheldon Ort	Manager IT – Risk, Compliance and Process Eli Lilly and Company
Charles Palmer	Chair and Director of Research I3P, Dartmouth College
Shari Lawrence Pfleeger	Senior Information Scientist RAND Corporation
Roberta Stempfley	CIO Defense Information Systems Agency (DISA)
Phil Venables	Managing Director and Chief Information Risk Officer Goldman Sachs Group
Lee Warren	Chief Information Security Officer United Technologies Corporation

Center for Digital Strategies Team Participants

Ajit Appari	Senior Research Fellow
Jennifer Childs	Program Manager
Jeff Moag	Writer
Ling Xue	Senior Research Fellow
Xia Zhao	Senior Research Fellow
Zach Zhou	Senior Research Fellow