



The Intersection of Business & Security

Human Behavior and Security Culture

A Workshop Overview

U.S. Chapter Discussion



Human Behavior and Security Culture

Managing Information Risk through a Better Understanding of Human Culture

An Executive Workshop for CISOs

A workshop for information security executives convened July 19–20, 2011, to examine information security risks and challenges posed by human behavior. The workshop included security leaders from Automatic Data Processing, Inc., Bechtel, Cigna, Cisco, Colgate-Palmolive, Eastman Chemical Company, eBay, General Dynamics, Goldman Sachs, L.L. Bean, the MITRE Corporation, Providence Health & Services, Praxair, Staples, Starwood Hotels & Resorts Worldwide, Stream Global Services, Time Inc., and the U.S. Department of Homeland Security, as well as academics from the Tuck School of Business at Dartmouth. The workshop was sponsored by the Center for Digital Strategies at the Tuck School and the Institute for Information Infrastructure Protection. The organizers wish to thank the attendees for their time and insights, and the Department of Homeland Security for its support.

Key Insights Discussed in this Article:

- **Culture is a security tool.** An organizational culture that values sound security practices is far more effective than regulations that simply mandate them. Information security executives can leverage cultural change by introducing security to company lore, employing a judicious mix of positive and negative examples, and using social media to create viral awareness campaigns.
- **‘Generation-Y’ is here, and gaining influence.** People entering the work force today are accustomed to working on a variety of mobile platforms and to storing and sharing data using cloud-based systems and social networking sites. They have a more permissive view of information-sharing than older workers, and they expect to work on their own schedules, with devices of their choosing, often from remote locations. All of these behaviors enhance risk, and they will become more prevalent and more difficult to curtail as Gen-Y workers continue to gain influence in their organizations.
- **Don’t manage the device, manage the data.** Faced with a tidal wave of consumer devices, workshop participants advocated data-centric security models. The “green screen” is back in vogue and Citrix has become everyone’s best friend, as companies herd data away from the endpoints to protected areas. Described as “Hotel California”, this strategy allows data to check out, but never leave.

- **Adversaries are becoming more capable, creative and persistent.** An increase in sophisticated social-engineering attacks and targeted malware has forced organizations to rethink human vulnerabilities. Adversaries are learning from their mistakes, exploiting new vulnerabilities, and when foiled, they keep trying.
- **Consumers persist in dangerous behaviors, and frequently resist help.** Education and awareness is of limited use with very large populations of users, and it's not possible to provide protected infrastructures to large groups of clients or consumers. To facilitate better security, consumers may have to take more personal responsibility and trade some privacy for security. Facing real consequences—such as financial liability for a stolen credit card—could help consumers develop better habits. So could clear, immediate feedback such as color-coded password warnings.
- **Teach employees to think for themselves.** Security is everyone's job and security executives are reaching for new ways to encourage employees to trust their judgment, and to question practices they believe may increase risk. This is particularly important for middle managers, who frequently make decisions weighing security risk against potential business gains. Some companies are training IT helpdesk personnel to take a more proactive role in security and security education.
- **A tidal wave of consumer devices.** New computers, tablets and smartphones enter the consumer market rapidly, and at progressively lower cost. Allowing workers to use these devices to access and store proprietary data creates added risk. Laws in many jurisdictions make recovery difficult. This trend is inevitable, and security efforts should be focused on managing the safe use of these devices rather than limiting them.
- **Vulnerabilities Extend Beyond Laptops, Tablets and Phones.** A host of IP-addressable systems, from building-control systems to remote cameras, constitutes a broad second front in the information-containment fight. The integration of systems across platforms, such as iPods that plug into vehicle entertainment and navigation systems, create added risk.
- **An end of complacency?** A wave of highly publicized hacks and data leaks in the last 18 months has raised the profile of information security. As a result, the public has become more aware (and perhaps more accepting) of information and privacy risks, while leaders in government and the private sector appear to be giving the issue more attention.

Introduction

The last 18 months has seen an explosion of high-profile data breaches, from the HBGary takedown to the Sony PlayStation hack and, most notoriously, the WikiLeaks case. While the public may imagine these cases to be the work of brilliant super-hackers coding through the night, the truth is more pedestrian: Each exploited human factors. The HBGary takedown hinged on the victims' deplorable computer hygiene and the astonishing credulity of one executive, while WikiLeaks was the work of a disgruntled U.S. Army Private with an extraordinary degree of access. Even the largest and most sophisticated breach yet known—the widespread penetration of U.S. and foreign agencies and defense contractors in a six-year effort believed to be backed by a foreign government—reportedly relied heavily on social engineering and other human exploits.

These cases offer vivid proof that corporations and governments today face great risk from members of their own organization. Whether willful or inadvertent, vulnerability to human-induced leaks is increasing. A flood of consumer devices is inundating the workplace, changing the way employees access, use and share company information. Maintaining information security promises to become more challenging as the new generation of “digital natives” gain influence in the work force. So-called Gen-Y workers share compulsively through online social networks, move more frequently among jobs, and use an array of devices, both in the office and at home.

These shifting work habits coincide with an escalating threat. Attacks targeting individuals are growing more sophisticated and persistent. The market for illicit information is more active and organized than ever, so that stolen data are more easily moved and more readily converted to cash. The ability to quickly disseminate information via social media, without regard for the gatekeepers of old media, is an incentive for activist hackers. Human-induced leaks, compounded by mass distribution through organizations like WikiLeaks, can create tremendous exposure. Not even Julian Assange is immune. After a falling-out with his team of merry hacktivists, his carefully guarded trove of stolen files was stolen by a former confidant.

A Confluence of Human Threats

Organizations are made up of people, so human-factor threats are pervasive at all levels. Security and IT professionals make decisions every day that balance security against the imperative of making the business work, said Christopher Dunning, CSO at Stream Global Services Inc. Technical teams often have their own ideas of how to implement security, and resist being told how to implement security. Line workers use compliance to justify controls and processes that may not be needed, or that result in a static defense posture rather than a dynamic one. Leadership presses to speedily adopt new devices, often with an executive mindset that Dunning describes as “make it work easy for me, and make it so I don't have to have a password.” Finally, you have the arrival of Gen-Y, the digital natives who have a propensity to “as John [Stewart] said, ‘click on every link as fast as they can,’” said Shamla Naidoo, Vice President for Information Risk and

Security at Starwood Hotel and Resorts. “These are the people that are growing into the corporate structure who are going to be the executive decision-makers in just a few years,” she said.

Given that some degree of human-related risk is inevitable, the best way to mitigate it is to structure the organization so that no single person can cause critical damage, said Philip Venables, Managing Director and Chief Information Risk Officer at Goldman Sachs. “If ever we see situations, or near situations, in which we’re relying on one person doing something, or not doing something, then that’s a trigger to look for better more systemic control approaches,” he said. “We’re doing less on staid approaches to training and awareness—i.e. less emphasis on coffee cups that say ‘Think security’ and mouse mats that tell people how to change their passwords—and more emphasis on process-integration and process-design—really equipping the enterprise to be risk managed by all people,” Venables said.

Moderator Eric Johnson, Director of the Center for Digital Strategies at the Tuck School of Business, described a three-phased security strategy comprised of controls that take people out of the loop where possible; effective training and awareness; and strict data controls. “We call it the Hotel California scenario—you can check out any time you want but you can never leave,” he said. In this approach, all data that leaves the enterprise must be user-authenticated.

Generation-Y is Here, and Gaining Influence

The influx of “Generation-Y” employees into the work force presents a multifaceted security challenge, which will continue to grow as young, technology-embracing workers gain influence. The healthcare field provides an example of what’s to come as Gen-Y continues to assert clout, said Eric Cowperthwaite, CISO at Providence Health and Services. “I’ve got plenty of doctors who are 30 years old,” he said. “They are driving what we do, and they are bringing all of the good and the bad of Gen-Y into the workplace.” These doctors expect to use their iPad to access electronic medical records, receive email on their iPhones and work on whichever laptop they choose—all requests that Providence has met, despite enhanced security risk. “What are we going to do, tell those doctors, ‘Sorry, you can’t practice medicine with us because you want to use your iPad?’” Cowperthwaite said. “That’s just not reality.”

While healthcare may be farther along this path than other sectors, Gen-Y will bring significant changes throughout the workforce. Young employees want to work on their own schedules, often from home or remote locations, using devices of their choosing. They are less likely than previous generations to view employment as a long-term relationship. They have a more permissive view of information-sharing than their elders, and they are habitual users of social networking and other tools that place data at risk.

Without good education and awareness, Gen-Y employees are more likely to move confidential information to places it should not be, such as Google Docs, Cowperthwaite said. “That’s just normal to them. They’re used to having a laptop, a netbook, a tablet and

getting the applications they want by downloading from the Internet or accessing them from cloud devices.”

Sooner or later, some members of Gen-Y will find their way to the executive suite, said Naidoo. “We’re evolving into a very open society. If we don’t accept that reality now it will be forced on us by executive leadership as [Gen-Y] grows into those roles.”

A Tidal Wave of Consumer Devices

The current generation of executives has already embraced the wave of consumer devices flooding the marketplace, and the work habits those devices enable. Cowperthwaite recalled a meeting of about 120 top executives in October 2010, about six months after the iPad release, at which about half of the participants were using iPads. “So I quickly pulled out my own iPad and I sent an email to my team and said, ‘Okay, guys, time to figure out how to support iPads and iPhones, because the CEO has his out,’” Cowperthwaite said. The tablet computer and the smartphone have become ubiquitous, and at this point in time, the people most likely to have them are senior leaders.

According to some estimates, the number of Internet-enabled devices surpassed the world population last year. With that many platforms in circulation, the question is no longer how to avoid an influx of uncontrolled consumer devices, but rather how best to deal with it. The answer will certainly involve managing enhanced human-related risk, said Cowperthwaite. “In my opinion consumerization magnifies the reality that 80 percent of your information security risk is about people not things,” he said.

Storing proprietary data on employee-owned devices creates an immediate problem. Local laws vary, and are often unclear, about the lengths to which a company can go to recover information on an employee-owned device, particularly after the worker has left that company. As Ray Musser, Staff Vice President for Security at General Dynamics Corp., said, “He’s walked away with that device, turned it off, and we have no way to get back to it.” People have a tendency to think that anything they create belongs to them—even when it was developed for, and properly belongs to, their employer. When such people switch jobs, they may attempt to bring that intellectual property with them.

Many companies rely on contracts to protect their right to recover proprietary data. In July, Bechtel released a new Information Use Agreement that all employees are required to agree to, said Don Michniuk, Corporate Manager of Information Security at Bechtel. “It’s part of the log-in process now; you don’t get access to anything in our electronic world without having to read through that. It takes away all their domain to those devices. It says we can confiscate them at any time for a legal matter, like e-discovery.”

Bechtel, like many other companies, has noted a significant increase in the proportion of unmanaged devices relative to managed ones, Michniuk said. That shift has forced Bechtel to change the way it does security. Because the shift to unmanaged devices reduces the available technical controls, security efforts must rely more heavily on human

factors such as awareness, hygiene and organizational culture.

Participants shared a general consensus that the influx of consumer devices into their enterprises is inevitable. Johnson offered the metaphor of a tidal wave. “Some of us may already be getting very, very wet, and others of us might be just still watching the wave coming. But regardless of where you find the wave, are we really doing anything more than floundering?”

Cowperthwaite noted a dichotomy in outlook between the information security community and their IT counterparts. “The problem in many cases is not the information security folks, as we’ve gotten over our desire to build walls to stop things,” he said. “And in general I see the IT organization being incredibly resistant and trying to build dams to stop the tidal wave.”

Karen Carman, Director of Information Security and Services at Eastman Chemical Company, said that the industry has moved beyond the dam-building stage. “We may not like it, but everybody’s committed to managing [the widespread adaptation of consumer devices], both on the IT side and the information security side,” she said. Nonetheless, some security professionals feel that the industry is still finding its way. “We don’t have a clear pathway,” Carman said. “We’re doing some pilots and we’re consigned to the fact that we have to go in that direction, but we don’t feel good about where we are at this point in time.”

Adversaries are Capable, Creative and Persistent

Adversaries are becoming increasingly more sophisticated. Musser noted a general trend toward targeted attacks. He gave the example of a senior executive who received an email that appeared to be from their spouse. The spouse has a different last name, and several senior people were copied on the email, indicating a sophisticated social-engineering effort. The ruse was effective—the executive opened the email, then saw a problem and immediately reported it to Musser’s team. “We were able to stop it,” Musser said, but “seven days later they hit the executive again. Same type of tactic—a different email, but scripted all the same. They’re persistent.”

In this case, training and awareness averted a potentially damaging breach. Dave Cullinane, the CISO at eBay, shared a similar anecdote. At his CEO’s request, Cullinane had given an information security presentation to senior executives. “And literally the next morning the head of HR forwarded me an email and said, ‘Yesterday I would’ve clicked on this, but after listening to you yesterday I figured I shouldn’t click on anything,’” recalled Cullinane, who forwarded it to his resident malware expert, who discovered “an incredibly sophisticated Trojan would have been downloaded if the user had clicked on the link.” Musser said that General Dynamics emphasizes employee training as a major component of its defensive strategy against such attacks. As the black-hats improve, however, so must the training.

“The adversary is getting better and more innovative all the time,” said Roland Cloutier, Chief Security Officer at Automatic Data Processing, Inc. They also are learning from their mistakes. Targeted malware attacks are now using telephone numbers cloned from the target’s business accounts, for example, because earlier attacks failed when the target became suspicious of an unfamiliar number, Cloutier said. “It’s hard enough for us to keep up with that; it’s impossible for the consumer to keep up with it. And every day there’s a new change, so how do you continue to educate them?”

Teaching Employees to Think

Building a sound process is an essential component of good security. But no process will protect a company against employees who fail to think. For example, sometimes a process or procedure is changed to make it more secure only to have employees later resume an old, less-secure approach—either because training materials were not updated or organizational memory resurrected the old way of doing thing. “We’ve started to ever-more remind people to say, ‘Look, trust your judgment,’” Venables said. “If you think something’s wrong or sub-optimal, just put your hand up and ask, ‘Is this the right thing to do?’”

Such training is especially important for middle-managers, who are often called upon to make decisions balancing security needs against other business priorities. Shari Lawrence Pfleeger, Director of Research at the Institute for Information Infrastructure Protection, noted that corporate incentive schemes often favor efficiency over security. “The rewards system in an organization clarifies in some way what the important goals are,” she said. “If you don’t get rewarded for security but you get rewarded by delivering your application on time, then you take [security] shortcuts to get your application done,” she said.

Leadership frequently exerts similar pressure. One participant noted that their senior executives are bringing in the technology now and basically saying, ‘Make it work. Make it secure.’ Tellingly, John Stewart, Vice President and CSO at Cisco Systems, noted, the request is typically framed in that order: Make it work first. Then make it secure.

The helpdesk can also be effective in encouraging good security practices throughout the company, Venables said. He used the analogy of a hotel concierge, who not only makes reservations at the best restaurant, but also advises guests to avoid streets on which they’re likely to get mugged. Goldman has implemented this approach and now has a Technology Concierge team that is much of a trusted advisor on use of technology as a classic help desk.

The Intersection of Innovation and Security

Innovation is frequently at odds with good security practices. The same factors that can help an enterprise profit from new technology—rapid adaption, innovative uses—often

create added risk. There's little doubt which side the leadership chooses; corporations are in the business of generating profit. Anything that stands in the way of that is at a cultural disadvantage.

“In that kind of an environment where people are being encouraged to bring new ideas forward, they have to have a fundamental understanding of why security is important,” Cullinane said. “Otherwise they're going to create major problems.”

Cullinane gave the example of a mobile application with tremendous profit potential for eBay. The application generated half a billion dollars in revenues in the first eight months, and is projected to generate more than \$2 billion in 2011. However, security for the mobile environment is something that is still being defined.

When some colleagues at Goldman Sachs questioned Venables' conservative approach to new potentially riskier technologies, he answered that his role is to be conservative. “My response was, ‘My job is to lock things down. If you don't want that to happen you've got to create another side of that equation—somebody that's going to advocate for flexibility, usability, and innovation so that we can balance these things by broader management debate rather than have one person internalize the risk process,’” he said. Goldman then created a so called “Green Light Committee” tasked with clarifying and revalidating legal, compliance and security obligations that if interpreted incorrectly could stifle innovation. This helped everyone get shared perspective on the challenges and the risk decisions which not only led to better outcomes but also a more continued productive dialog. CISO's have a multifaceted role that is unique in many organizations, noted Cigna Corporation CISO Debra Cody. “In the CISO role you see the convergence of a multitude of internal corporate perspectives, specifically legal, fraud, special investigations, compliance, privacy, employee relations, and last but certainly not least, the business segments that you support.” The confluence of these perspectives presents CISOs with unique challenges, she said. “You take it for granted that those you interface with also have a similar convergence, and that they understand your challenges. And in fact they don't.”

Culture is a Security Tool

Several workshop participants noted the power of organizational culture. Stories shared around the water cooler can influence awareness and behavior in a way the formal training rarely does. Stewart gave the example of a 22-year-old contract worker in a Cisco call center who received a call from someone claiming to be Cisco Senior Vice President (now Executive Vice President of Sales) Rob Lloyd. The caller was insistent that the young woman provide privileged information, but she held her ground, even as the impersonator berated her and threatened to fire her. She hung up and immediately reported the call to Stewart's team.

“Rob's response was to say, ‘I'm being impersonated. That's great.’ He tells his whole team as if it's the coolest thing since sliced bread that he was impersonated,” Stewart

said. As a result, “his whole team completely absorbed that message in an amazingly in-depth way.” No employee education effort could have had the same effect. The story spread virally through the company, carrying with it an essential message—to be wary of social-engineering efforts.

Negative examples can also find their way into company legend. Stewart shared another anecdote that he often tells within his company. An employee had illegally downloaded a television series from a file-sharing site. Stewart called the person in to remind him that such downloads are illegal, and moreover he’d signed a business contract forbidding him to do so. The worker apologized and promised to delete the program from his hard drive. “I said, ‘Don’t worry. We’ve already deleted it off your computer,’” Stewart recalls. That should have been the end of the story, but the next day the employee downloaded the series again. Stewart terminated him immediately.

“We walked him out, because if you cannot learn from a personal conversation then you’re never going to be someone I’m safe with,” he said. “That story is very effective within the company, because it shows that one-time mistakes can be forgiven, but not repeated transgressions.”

When Donna Lamberth started her career 20 years ago, at Time Warner, she learned immediately that the company had zero tolerance for any transgressions involving intellectual property. “Everybody that I met in my first week on the job had a story to tell about that guy who was fired on the spot for a transgression,” she said. “It was clear and simple, and people really didn’t violate that.”

Robert Duran, Vice President of Information Risk Management at Time Inc, seeds his company culture with cautionary tales, using examples from inside the company. “I’ll hold meetings with departments, and I’ll talk about incidents that relate to them, and we’ll talk about the groups that were involved in those fiascos,” he said. “That’s a way to sort of let them burn their hands without letting them burn their hands. Public embarrassment does work to a certain extent.”

Shaping security culture outside the enterprise is much more difficult. Certainly everyone agreed that it is important to have airtight contracts, and then to “trust but verify, with a big emphasis on the verification,” said Pfleeger. The group had little confidence in auditors, who they see as having a checklist mindset. Instead, companies should conduct more thorough assessments of potential partners. It also is important to publicly and aggressively enforce the terms of the contract. Some argued that you should “shoot the transgressors” and then let the others know that you did and why you did it.

Inside the organization, a softer touch is sometimes called for. Deanna Caputo, Lead Behavioral Psychologist at Mitre Corp., noted the value of inviting employee family members to trainings—an insight that Hans Brechbühl, Executive Director of the Center for Digital Strategies, noted also came out of the human-related risk workshop the Center sponsored in Europe in June. Including family is particularly relevant given the continuing breakdown of the work/life divide, and the increasing likelihood that children

and spouses will use devices employees use for work.

Participants reported success with shorter, more frequent training periods and an emphasis on fun, memorable techniques. “One company used puppets, and the employees loved it,” Caputo said. The European conference also generated a similar insight, Brechbühl said. Swiss Re produced a coffee-table book featuring photos of animals, together with very short messages about security. “They had animal posters as part of the campaign, like two beavers lying in a stream on their backs saying, ‘Why should I care?’” Brechbühl said. “They were really appropriate for the theme and very eye-catching.”

Goldman has found similar success by changing the tenor of warning pages that appear when employees try to access blocked websites, Venables said. “We made it a friendlier message that said, ‘Unfortunately we’ve not been able to get you here. We understand you may have a potentially valid reason for doing it, but we’re not going to let you go there for these reasons of risk and policy listed below,’” he said. The message concludes by thanking the employee for helping protect the firm and its clients, and provides a link so that they can share the warning with colleagues for their benefit. They found that many people shared the message, especially among the Gen-Y segment of employees.

Paradoxically, social media has proven to be a powerful tool for educating people about the risks of social media. Cisco produced a series of comic videos, the first of which was about the consequences of losing a laptop. The clip went viral throughout the company, and when Stewart’s team announced they would end the series after three videos, employees protested. “We’re giving up on the very traditional ways of delivering” security education, Stewart said. Instead, Cisco is using a number of Gen-Y friendly means to spread the message, some of which are humorous. The campaign includes text messages, testimonials of colleagues who have been hacked, and presentations by the likes of Frank Abagnale, the con-man turned security consultant whose life story became the Hollywood thriller “Catch Me If You Can.”

Helping Consumers Protect Themselves and the Enterprise

Enterprises that deal with large numbers of consumers or clients face particular challenges. As Cloutier said, education is a powerful tool “but what if you have 60 million users?” Such a large number of users can’t be confined to a protected infrastructure in the same way that workers at large firms and government agencies can be. Goldman Sachs provides some clients with that type of protection. The program came about because some clients needed assistance in maintaining a more tightly controlled environment; this was an extra service Goldman Sachs could provide. It wouldn’t scale to 60 million users. In addition to the technical hurdles and need for training, the cost would be prohibitive. “It’s getting so you need to have a very sophisticated security organization to be able to deal with the threat,” said Cullinane. “Most companies can’t afford a very sophisticated security organization.”

Some workshop participants suggested that the public expectation of privacy and security is not realistic, given the nature of the threats and the high cost of countering them. Placing the security burden solely on business is therefore not realistic. Nor is it reasonable to expect consumers to read and understand and accept their security responsibilities. As Time Inc.'s Duran said, "I read [a privacy agreement] and it makes my head hurt, and I'm part of writing the solution."

The public has an incorrect assumption that security is built-in, said Roberta Stempfley, Acting Assistant Secretary for Cybersecurity and Communications at the U.S. Department of Homeland Security.

Consumers "essentially have no pain point that causes them to change behavior," said Stewart. "You got your credit card stolen because you used it everywhere. But don't worry, no pain to you; we've got you covered."

This lack of pain is especially prevalent in the United States, said Naidoo. "In many countries, when you take your credit card out of your wallet, you take the personal risk and you absorb the consequence of that action. But in the U.S. someone else owns the responsibility. Someone else has to make me whole for whatever irresponsible, reckless and careless behavior I might apply."

Often, businesses are effective in protecting consumers. Musser related a recent cell phone call he received from an American Express representative who asked whether he was in New York. "No, I'm in Falls Church," Musser replied, to which the AmEx rep answered, "Well, there's somebody in a Rite Aid right now in New York City trying to buy \$44 worth of goods and services." The point, Musser said, is that technology does exist to protect consumers from many types of fraud. The catch is that consumers must exchange some degree of privacy for that protection, Cloutier noted. Many are unwilling to do so.

Cullinane said that the vast majority of compromised accounts he sees are the result of malware on the user's computer. Yet even when eBay arranged to provide Microsoft Security Essentials to customers free-of-charge, many resisted. "We had a focus group with a bunch of customers and literally had these silly discussions with people, 'My son takes care of my security so I don't need your help.'" Cullinane said. "We finally got her to download MSE, and she had dozens of infections."

Teaching consumers to recognize risk is a large part of the challenge. Clear, simple and immediate feedback can be remarkably effective with consumers, said Praxair CISO Ram Hegde. "When users get feedback about passwords—rating them red, yellow or green—that's 1,000 times more effective than just telling them, 'Choose a complex password,'" Hegde said. When systems are designed to give the appropriate feedback and to correct user behavior, users are more likely to adopt good practices, he said.

Social Media Teach and Facilitate Compulsive Sharing

Social media has quickly become a powerful tool for business. Executives measure brand-building efforts by the number of Facebook “likes” and Twitter followers their companies attract, and the immense valuation of social networking sites is testament to the marketing muscle they wield. Social networking makes it easier than ever to share information. What’s more, said Cloutier, these sites encourage it. “Facebook is actually teaching people to share. That’s their mantra. Social networking is breaking down barriers about what we say and show. That’s the impact it’s having on the flow of information.”

In some respects, social networking comprises only one facet of a larger problem, said Cowperthwaite. “I don’t necessarily see social media as separate from the data-loss issues of living in the electronic world,” he said. “Google wants you to live your entire electronic life in the cloud. Their goal is for your computing device to be the terminal that lets you access Google Docs, Google +, Gmail, etc. And I think that that reality is coming.”

Vulnerabilities Extend Beyond Laptops, Tablets and Phones

Connected devices are no longer limited to computers and smartphones. Stewart noted the proliferation of IP-addressable systems throughout his enterprise, from building-control systems to IP cameras, audio systems, and flat-panel displays. Beyond the challenges of Gen-Y and consumer devices, information security practitioners must contend with an “unbelievable amount of IP-addressable stuff that doesn’t have any of the protections, but that has an Ethernet and a job integer, or a Flash-based integer or an operating system,” he said. Household power meters and even refrigerators are now routinely connected to the internet. So are automobiles. Stempfley described a conversation that the Department of Homeland Security has had with executives at Ford. “They’re being driven by Apple because every car driver wants to connect their iPod into the infotainment system in their car, and we’re telling them, ‘Please make sure the infrastructure for that is completely separate from the data bus that runs the car.’”

OnStar, the GM service designed to provide motorists with directions and other assistance, including remotely unlocking vehicles, disabling their throttles, and blocking their ignition, presents a particular security challenge, said Duran. “OnStar is fascinating, especially with the capability to stop your car now. If somebody took that over, they would be able to just shut down the freeways.” That scenario has already played out in at least one instance, Stewart said. “A kid in Texas was being fired from a car dealership. He had all the codes, and he called OnStar and said, ‘Shut the cars off.’ Something like 70 cars were shut off in mid-flight.”

Potential Cost Savings Of Uncontrolled Devices Prove Elusive

There could be some business advantage in moving to uncontrolled devices. Several companies represented at the workshop have analyzed the potential cost savings of such a shift, with varying results. Providence is bullish on this strategy, Cowperthwaite said. “We are moving toward a model where we limit our management of the consumer device to requiring specific security controls are put in place. Rather than a full management lifecycle, we will instead maintain and manage the virtual environments that we allow to run on the devices. Our belief is that [this approach will be] significantly cheaper and more secure than trying to manage or maintain our approximately 10,000 mobile end-points,” he said. Because the cost of back-end software and other expenses will likely offset acquisition-and-support savings, Staples determined that uncontrolled devices will “come out a wash” relative to managed devices, said Charles Burns, Director of Worldwide Security and Enterprise Architecture at the office-supply retailer. Cisco studied the potential efficiencies and concluded that unmanaged devices are more costly, due to additional risk exposure and the fact that employees routinely call the helpdesk to support their unmanaged devices. “Folks are buying [a device] and then coming back wanting it to be managed,” Stewart said. “We’re having to chase down a phenomenal amount of data that’s not properly backed up, using forensic techniques that are expensive because we don’t have the natural infrastructure” of a managed environment.

On the positive side of the ledger, the freedom to use consumer devices may make employees more efficient, Cowperthwaite said. Access to the slickest new devices may also aid in recruiting, morale and retention. Cowperthwaite used his personal schedule to illustrate this point. In the past, he would spend about an hour at home each evening, attending to company business on his laptop. “Now with a smartphone in my hand I’m taking care of all of that email throughout the evening really quickly without impacting significantly my family life,” he said. Pfleeger cautioned not to confuse working more with working well. Citing a recent *New York Times* story, she noted that some studies are showing that people who multitask are not as productive or creative as their less-distracted colleagues.

The Best Defense is a Good Offense

Catching and punishing a bad actor after the fact is by definition a Pyrrhic victory; the goal is to prevent bad things from happening. To that end, monitoring tools can be used to identify insiders who fit patterns consistent with illicit activities. “The cases we’ve had with bad insiders, they have what I call bad IT hygiene, because they’re doing stuff all the time and rules are not for them,” Musser said. “It shows in what they do.”

More sophisticated reporting tools give security people better visibility into data movement and employee activity throughout the organization, Johnson said. “These tools are able to signal to management that ‘20 percent of your users are routinely shooting things to Hotmail. Is that an issue or not?’” he said. Tools such as next-generation

firewalls that allow greater visibility about where people are going, and why, can have powerful security applications, Johnson said.

Legally speaking, monitoring employees often treads a fine line, said Cody. “It’s a balancing act between violating individual rights or doing targeted monitoring versus having policies that you can support in court or are applicable to anyone in a particular situation,” she said. “For example, if we notice that people are sending their personal internal résumés home, that’s a flag, and then we do across-the-board monitoring for those individuals.”

Cigna also monitors people on its internal future termination list, Cody said. “We apply particular optics to those individuals for the duration of their tenure to make sure that unwanted behaviors don’t start occurring,” she said.

Dunning noted another problem: people who come to work at a company in order to infiltrate it. Stream Global Services has 50 call centers in 24 countries and “there’s a percentage of people who are hired in those call centers with the clear goal to steal,” he said. “That’s why they go there—to steal. So the education and the awareness is irrelevant. It’s about catching them.”

A Race to Implement Existing Solutions

The security profession had been fairly quiet in the period between the worm scares of 2003 and 2004 until about 18 months ago, when news of Anonymous, LulzSec and APT penetrations began grabbing headlines. Some organizations may have been lulled into a false sense of security. In 2008, when news broke that hackers had stolen 4.2 million credit- and debit-card numbers from the Hannaford supermarket chain, Donna Lamberth recalls driving past one of the stores and seeing it nearly deserted at 6 p.m., when it should have been bustling. However, three years later, “I think the response to those kinds of situations by consumers is lessened because people have gotten desensitized,” said Lamberth, Director of Information Systems Services at L.L. Bean. Executives, on the other hand, are becoming more attuned to such risks. “I’m finding that my job is getting a little bit easier because people see [security breaches reported] on the front page of the *Wall Street Journal* and they’re saying, ‘Wow, we really need to invest in some preventive measures so that that’s not us,’” Lamberth said.

Cloutier made the point that in comparison to such challenges as Advanced Persistent Threats, the risk posed by mobile connected devices can be managed more effectively. One solution may be to keep data in-house, and make it accessible by any device, said Naidoo. “It seems to me like we’re evolving and going back to the old days of the green screen,” she said. “Suddenly Citrix has become every corporation’s best friend when it comes to these mobile devices. So if you don’t want to manage the device, then you keep all the data in a platform that is insulated from those devices,” she said.

The tools do exist to contain the risk, agreed Stewart. The problem is implementing it as rapidly as the threat advances. “This is not a technology problem; it’s a speed-to-capability problem. I haven’t gotten fast enough to handle the risks created by the devices,” he said. Nonetheless, Cisco isn’t waiting for Stewart and his staff to catch up. “Our corporation just took a lot of risks; we said, ‘We’re going to fly right into this and if it’s a blender we’re going to run into it, and if it’s a swan song of productivity we’re going to run into it,’” he said. “We just leapt right off the cliff.”

Cisco is not alone; its aggressive adaption of new technology is more the rule than the exception in American business. That approach poses a formidable challenge for security professionals. The greatest challenge with regard to consumer devices is a lack of understanding, noted Cowperthwaite. “From a risk perspective I don’t think we yet totally understand what consumerization plus what we’re calling cloud computing is going to mean from an IT-management and information security perspective,” he said. In such a fluid technology environment, Cullinane said, “We need to be even more agile and innovative than the business is.”

That imperative applies to the larger problem of managing human-related risk at a time when technology and business practices are rapidly evolving. If information security were merely a matter of building better systems, it would be a simpler and far less interesting task. Instead we are dealing with the most powerful and unpredictable computer of them all—the human mind.

Participant List
Human Behavior and Security Culture
July 19–20, 2011

Charles Burns	Director, Worldwide Security and Enterprise Architecture Staples, Inc.
Karen Carman	Director of Information Security & Services Eastman Chemical Company
Roland Cloutier	VP, Chief Security Officer Automatic Data Processing, Inc.
Debra Cody	Chief Information Security Officer Cigna Corporation
Eric Cowperthwaite	Chief Information Security Officer Providence Health and Services
Dave Cullinane	Chief Information Security Officer and VP eBay Inc.
Don Dudley	Director, Global Security and Privacy Staples, Inc.
Christopher Dunning	Chief Security Officer Stream Global Services Inc.
Robert Duran	Information Security and Privacy Officer/VP of Information Risk Management Time Inc.
Mary Erlanger	Director, Global IT Risk Management Colgate-Palmolive Company
Ramachandra Hegde	Director, Global Information Security and Chief Information Security Officer Praxair, Inc.
Donna Lamberth	Director Information Systems Services L.L. Bean, Inc.
Don Michniuk	Corporate Manager of Information Security Bechtel Corp.

Ray Musser	Staff VP – Security General Dynamics Corp.
Shamla Naidoo	VP, Information Risk & Security Starwood Hotel & Resorts Worldwide, Inc.
Roberta Stempfley	Acting Assistant Secretary, Cybersecurity & Communications U.S. Department of Homeland Security
John N. Stewart	VP, Chief Security Officer Cisco Systems, Inc.
Philip Venables	Managing Director and Chief Information Risk Officer Goldman Sachs Group, Inc.

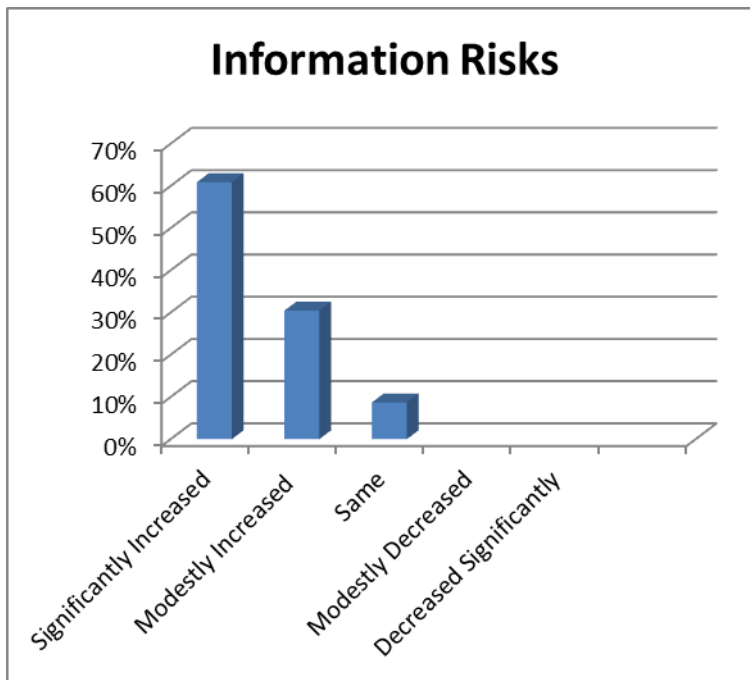
Tuck/I3P Research Team

Justin Albrechtsen	Senior Applied Psychologist Mitre Corp.
Ajit Appari	Research Fellow Center for Digital Strategies
Hans Brechbühl	Executive Director Center for Digital Strategies
Deanna D. Caputo	Lead Behavioral Psychologist Mitre Corp.
M. Eric Johnson	Director, Center for Digital Strategies and Benjamin Ames Kimball Professor of the Science of Administration
Juhee Kwon	Research Fellow Center for Digital Strategies
Shari Lawrence Pfleeger	Director of Research Institute for Information Infrastructure Protection

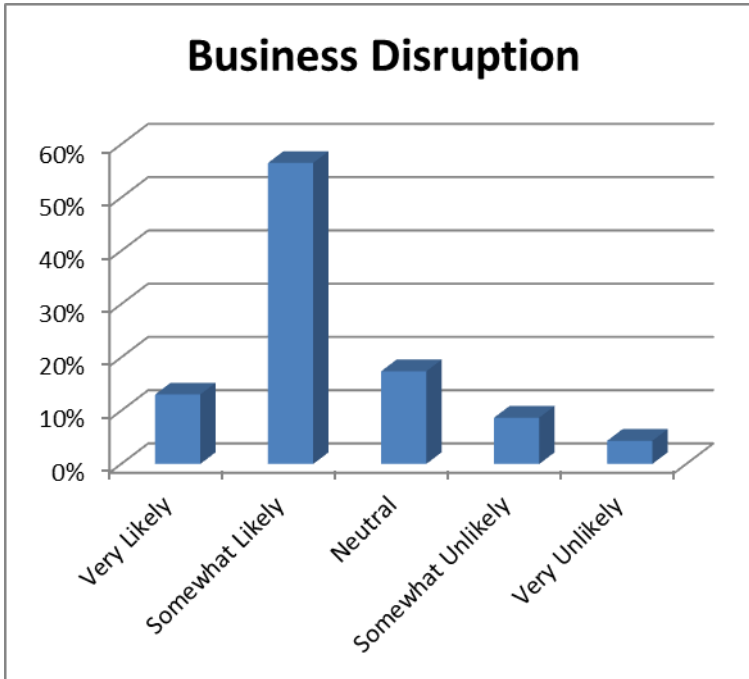
Appendix 1: Results of participant survey

A survey given at the outset of the workshop revealed that over 90 percent of the 23 Fortune 1000 CISOs consider human-related risk to be more troublesome than technical challenges in their organizations. The security executives believe information risks have increased in the last year, and most think that their organization will experience a significant breach in the coming year. While they believe that the US government largely understands the risks, they feel it is not devoting sufficient resources to the problem. Awareness is better inside the enterprise: 70% have received increased company resources to combat information risk.

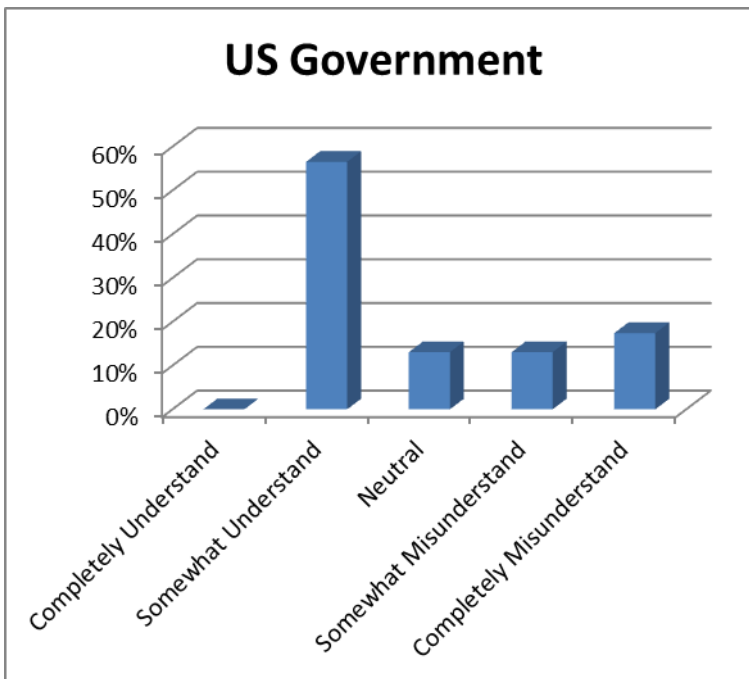
Over 90% said that information risks have significantly or modestly increased in the past twelve months.



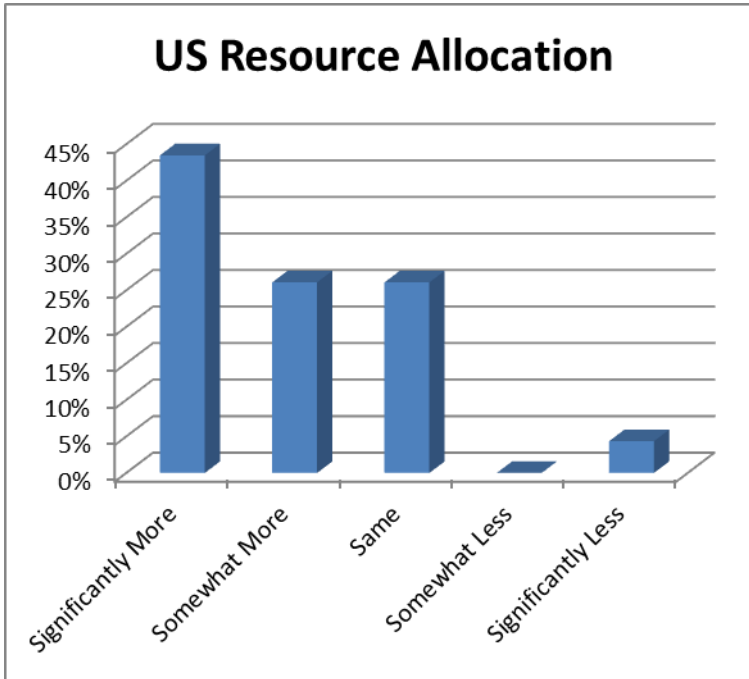
Nearly 70% feel that it is at least somewhat likely their firm will experience a significant cyber disruption or breach in the next year.



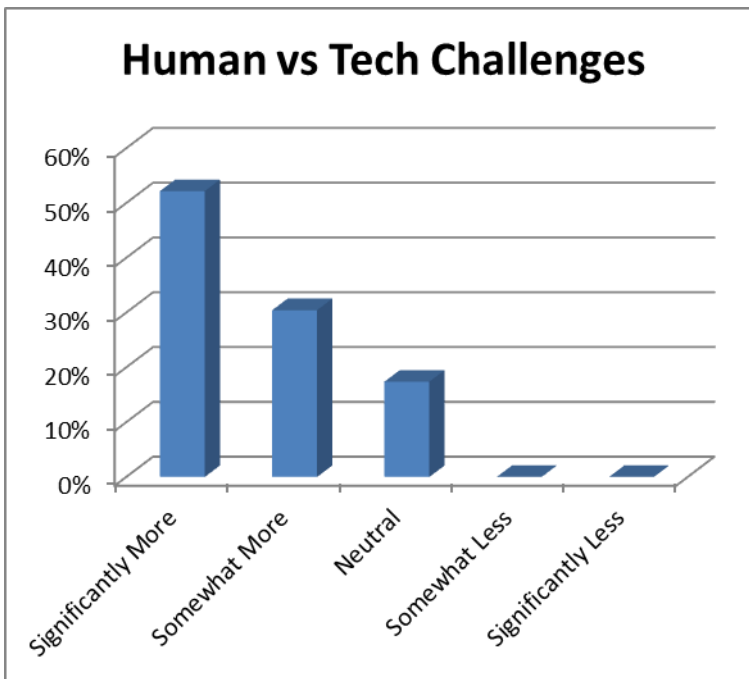
Most feel that the US government appreciates the risk, with only 30% saying they feel that the US government doesn't understand the information risks to business.



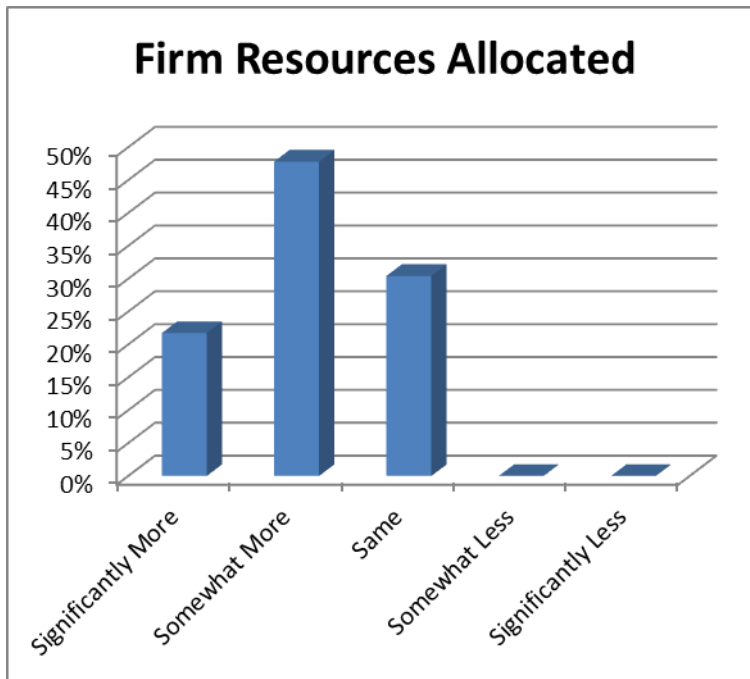
Nearly 70% feel that the US governments should allocate more resources to address information risk with more than 40% saying it should be significantly more resources.



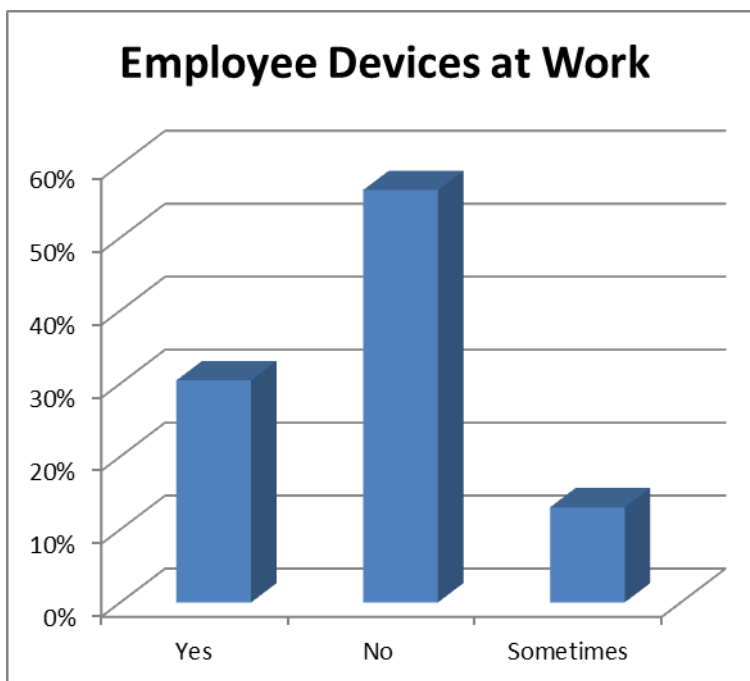
Of the information security challenges they face, over 80% feel that the human related risks are more troublesome than the technical challenges.



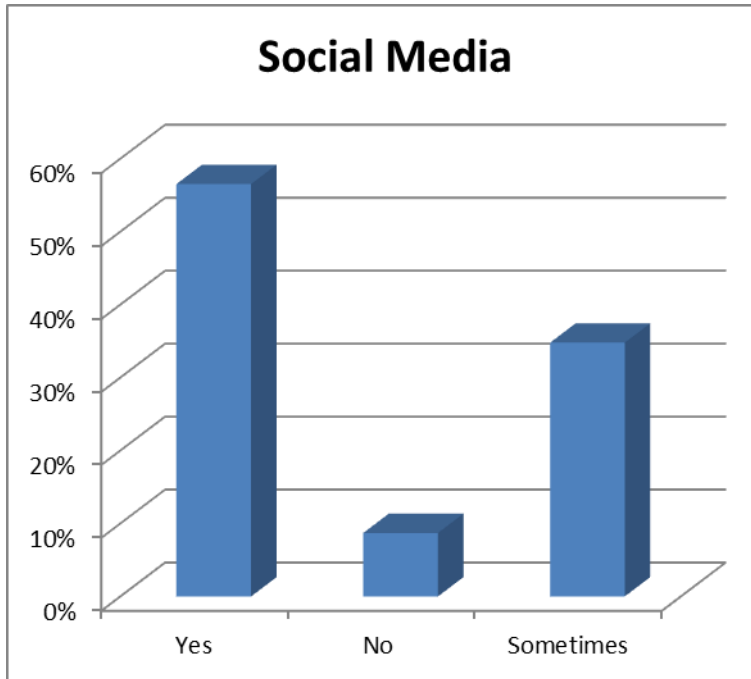
70% have been allocated more resources to combat information risks in the past 12 months, with none reporting cuts.



Most place limits on devices employees can bring to work.



Most allow employees to access social media sites from work.



Over 40% are now conducting social engineering attacks to test employees.

