TUCK SCHOOL OF BUSINESS AT DARTMOUTH
GLASSMEYER/MCNAMEE CENTER FOR DIGITAL STRATEGIES

Rethinking Cyber/Information Security

A Roundtable Overview

Americas Chapter Discussion

Roundtable on Digital Strategies

Rethinking Cyber/Information Security

Thought Leadership Roundtable on Digital Strategies
An executive roundtable series of the
Center for Digital Strategies at the Tuck School of Business

The Americas Chapter of the Roundtable on Digital Strategies convened at Bechtel Global's facility in Reston, VA for a day-long discussion of the current topics and challenges in information security. Cybersecurity has been a recurring topic in Roundtable discussions, as evolving technology continues to enable new business models, which in turn open up new vulnerabilities and new sources of threat.

The day began with a discussion of the catalysts of these linked developments and what they mean for real-life operating decisions to manage the security of digital information. Topics ranged from the new sources of cyber-threats to the changing realities of network intrusions to the solutions that will have to be developed in order to deal with the threat landscape: in technology, in policy, and in operations.

Participants included CIOs and their information security colleagues from host Bechtel Global Corporation, Eastman Chemical, Coca-Cola Enterprises, Tenaris, Time Warner Cable, and YUM! Brands, as well as cybersecurity legal expert Adam Golodner of Kaye Scholer. The session was sponsored by the Center for Digital Strategies of the Tuck School of Business at Dartmouth College, and moderated by M. Eric Johnson, Dean of the Owen Graduate School of Management at Vanderbilt University.

Key Insights Discussed in this Article:

Introduction: Cyberspace Will Never Be Completely Secure

Anonymous. Stuxnet. Target. Edward Snowden. These are names and terms familiar from the daily headlines.

Shamoon. Dark Seoul. LulzSec. The Elderwood Group. Unit 61398[1]. Terms perhaps less familiar to those who are not responsible for providing cybersecurity every day, but just as famous, and just as worrisome, inside the information security community.

Together, they represent the threats and fears that CIOs and CISOs have to identify and counter every day: advanced persistent threats, distributed denial of service attacks, hactivism, cyber-terrorism, cyber-theft, disgruntled employees, and exploitation of ever-increasing numbers and varieties of network vulnerabilities. The members of the Roundtable were not alone in putting focused attention on the topic: As they converged on Reston, Martin Giles of *The Economist* neared completion of his 2014 Special Report on Cyber-Security, "Defending the digital frontier." In this report, Giles addressed many of the same topics that engaged the Roundtable: The changing nature of the IT threat landscape, including the rise of state-sponsored cyberespionage; the rising costs — to individuals, corporations, and countries — of security breaches; the need for special protection of critical national infrastructure that is owned and operated by private enterprises.

Solutions, both Giles and the Roundtable observed, are not easy to come by: "Blocking sophisticated and highly targeted attacks is extremely difficult."[2] Beyond the headlines, the numbers assembled by Giles support this conclusion:

> When CDS last addressed cybersecurity at a CISO workshop in June 2012[3], 232 million identities had been exposed through cybercrime in the prior year. In 2013, the number of compromised identities exceeded 800 million.[4] As this article goes to press, the New York Times claims that a Russian gang has amassed more than one billion internet passwords.[5]
>
> The *mean* amount of time that hackers managed to continue operating inside compromised networks is 229 days; one group lasted six years[6]. And these calculations represent only those groups that have been caught — the true average network penetration probably lasts much longer.

All in, global spending on information security this year will exceed $70 billion, with annual damage from breaches estimated at $445 billion.[7] Solutions to these issues are critical: Governments, corporations, and consumers are all conducting more and more of their businesses and lives online, and they need to trust that the information and transactions are secure, private, and reliable.

---

[1] A real all-star in international cyber-spying: The intelligence unit of China's People's Liberation Army "credited" with hacking into at least 120 corporate networks since 2006. Source: Mandiant, cited in *The Economist*, Special Report on Cyber-Security, "Defending the digital frontier," July 12 2014, p. 8.
[2] Ibid.
[3] Center for Digital Strategies, *Cybersecurity: Risks and Mitigation. An Executive Workshop for European CISOs*. June 2012. http://digitalstrategies.tuck.dartmouth.edu/programs/ciso-detail/cybersecurity-risks-and-mitigation
[4] *The Economist*, ibid, p. 4.
[5] *New York Times*, August 5, 2014.
[6] *The Economist*, ibid, p. 9.
[7] Gartner ($70Bn); CSIS ($455Bn); both cited in *The Economist*, ibid, p. 4.

"It is not the strongest of the species that survive, nor the most intelligent, but the one most responsive to change." – Charles Darwin

No Walls High Enough

The Roundtable started its discussion with how and why the cybersecurity landscape has changed just within the last few years.

"When I took this role in 2010," began Siobhan Smyth, VP Information Technology Leadership, Coca-Cola Enterprises,

> Just protecting the periphery, protecting against denial-of-service attacks, was a big challenge. We've done a great job over the past few years of protecting our data centers, our networks, and the periphery from a technical infrastructure perspective. Now we are moving to mobile and social solutions and different third-parties in the cloud that don't have all the SAS-70 certifications that we expect, but we have to keep using these technologies to continue to lead in the marketplace. The challenge has shifted.

"When I first started in this job," echoed Keith Sturgill, VP and CIO of Eastman Chemical, "We had the illusion that we could be good enough to prevent getting breached. The really important shift in the last five years has been to the depressing idea that *when* we get breached, we have to respond and remediate quickly."

"It's not *if* we're going to be breached," Prentis Brooks, Director of Information Security for Time Warner Cable, agreed, "It's *when*. We're not going to be able to stop every attacker. So the point is, 'How do you deal with the event when it occurs?'"

Scott Catlett, Associate General Counsel for YUM! Brands, concurred: "Our walls cannot be high enough to keep out the bad guys. What we have to figure out is, 'What do we do when they get over the wall, so that at the end of the day, the steps we took will look reasonable and prudent for what we knew, when we knew it?' We've got to take prudent steps up front, but then once something bad happens, how can we assure ourselves that we've done the right thing?"

"What are the risks that have changed this discussion in the last few years?" asked Hans Brechbühl, Executive Director of the Center for Digital Strategies. "One is globalization; what are other chief challenges? What are the pieces that keep you awake, that open up risks that weren't there before?"

"Our largest goal/requirement is moving more towards digital," answered Carol Zierhoffer, CIO of Bechtel. "So that data becomes the currency of our processes instead of paper."

"Five years ago YUM! sold mostly in individual stores; now we are moving heavily towards digital channels," added Dickie Oliver, YUM!'s VP of IT.

> In China, 60 to 70 percent of our delivery business is online to some degree. As another example, it's a big milestone when a new store does $30,000 in business in its first week. On Super Bowl

> Sunday, we peaked at $32,000 a *minute* over our e-commerce platform. And our marketing groups and brands want to push the envelope even further with consumers.

"The stores want to build relationships with their customers now," explained Oliver's colleague Melanie Roush, Senior Manager of Global IT Risk and Compliance at YUM!:

> They want to track activity, to know how many times you're coming, to reward you. If you're on social media and talking about Pizza Hut or KFC, they want to be able to immediately recognize you, and provide rewards for doing that. We're going to be collecting more and more personal data, in all different countries. So how do we provide safe harbor in China, and comply with privacy laws in Japan? It's going to be very, very challenging.

Brooks added to Roush's point on social media:

> We all grew up with "Don't talk to strangers." This next-generation workforce will friend anyone. They've grown up on social media: "Let's share everything!" They don't have a good grasp of general security principles. Meanwhile we're moving away from the concept of "Here's my work; here's my home." Work and life are intermixed, so we're seeing really sensitive work stuff blended with personal stuff. And technology has not caught up.

Matt Looney, Director of Data Science & Enterprise Architecture at Eastman Chemical, connected social media technology and business model changes to security challenges:

> We don't just invent "stuff;" we invent stuff that people want to buy. So Marketing has connected with R&D, and they're trying to be more open than they've ever been. But Marketing people don't understand security, and we have lots of them who know how to use the world's technology to communicate and collaborate. And they don't want to use *our* collaboration platforms; they want to use consumer collaboration platforms.
>
> Because we've done a good job of securing our IT infrastructure, now they're working around us. One of our biggest challenges is to create a compelling experience with *our* infrastructure. The company's desire to do this faster has ratcheted up the complexity of protecting trade secrets.

"And that intellectual property," added Looney's colleague Sturgill, "Defines who we are. So our global network is now *the* strategic asset of Eastman Chemical: It's how we conduct business every day, how we communicate, how we ship product. We refer to it as 'the nervous system of the company.' We're even classified as 'Critical Infrastructure' by the Department of Homeland Security. Protecting that strategic asset from the bad guys is a front-of-mind issue."

Information Security Director Gustavo Diaz described a similar situation at Tenaris:

> The company has shifted from a manufacturing company, where the value was in the production and logistics, to a company where one of our most valued assets is the trade information about threads, the connections to other pipes. That's what we have to protect — but we also have to share that information, because some manufacturing is done by third parties. How do you balance sharing the information you need for your business to grow versus the risk that exposes you to?

The networks at Eastman and Tenaris have become critical infrastructure for those companies; Time Warner Cable's Brian Allen described an even larger scope of network security issues:

> We have a tremendous amount of credit card information and PII storage — those are always concerns. Interception of traffic — NSA-type stuff, by individuals or state actors — is significant. But for us, the big one is a service-oriented disruption. We service 17,000 911 calls per month just in New York City. Tie a disruption in with a terrorist attack, and that's a big impact to society. So we're facing heavy regulation, and that changes how we do business. And the regulatory bodies are not keeping pace with technology.

"Ten years ago we would have been worried about business continuity and business disruption," summarized moderator Eric Johnson of the Owen School at Vanderbilt.

> Two years ago we were talking about smartphones and BYOD. What we're hearing today is about the business changing. All the other pieces are still issues, but even though we may feel like we have technology locked down at some place, then the business shifts, and it opens up a whole new set of issues, whether from acquiring a company with different processes in place, or entering a new market, or the way we collaborate.

"It's a shift from cybersecurity being an operational issue to touching multiple strategic issues," suggested Alva Taylor, Faculty Director of the Center for Digital Strategies (CDS) and Tuck professor. "Businesses are starting to understand that, and it's shifting how we view these threats."

Target's Unintended Legacy

Sturgill emphasized Taylor's comment on the shift in perception of cyberthreats: "With all the Target issues, you can't read the *Wall Street Journal* for a week without seeing a major company being breached, so getting the attention of senior executives is a lot easier than it used to be, and that helps in what we are trying to do."

"Target was galvanizing," Oliver agreed.

> It got us attention at the levels of the board that we need. It's relevant to everybody's business: Target was just trying to drive a tighter P&L, engaging with a third-party. They gave credentials to the wrong person, who got breached, and all of a sudden chaos ensued. We *are* in the middle of something, and I don't know exactly what it's going to wind up being. But we've got to figure out how to engage our divisions and partner with them, so that we can stand in front of the Board and say, "This is our plan. This is our course of action. And we're able to go execute against it."

"But there are so many different scenarios that could materialize related to a breach or data loss," Smyth observed,

> And you never know what possible scenario is going to occur. One of the key learnings we've had is to have a good response management plan in place. More than that, you need to have a view of all the possible scenarios that could occur, and put in measures to prevent them. We look at what could

> happen in a denial of service attack, and how we could prevent it. What if someone infiltrates our supply chain systems? Anonymous is always threatening Coca-Cola…. Those are the obvious ones, but you can't get too comfortable that these are the only risks that keep you up at night.

"The Snowden sets of issues have super-charged those discussions," commented Adam Golodner, Partner at Kaye Scholer. "And it's not necessarily clear where all of this is going. We *will* end up with interoperable, secure, open, global networks. But there's a lot of hard work, and it won't happen without government and industry coming together to figure out the rules of the road."

"But our security industry is spinning its wheels in a lot of ways," Allen objected. "Defining what security is, and what its role is, needs to happen, because there's inconsistency. Great people are doing great work in a lot of great companies, but consistency is not there."

Brooks widened the aperture on the impact of security risks:

> We need to pay attention to the threats, but it's also making sure we have a plan to handle them. I don't mean just the technology piece of instant response, but also how do you loop in the executive levels and the executive communications?
>
> The biggest thing about the Target event wasn't that they were breached; it was the level of ramifications that followed. It wasn't that Target leadership was doing the wrong things in trying to protect their environment; it was how they handled the issue when they had the breach. It was the level of communication and response on how they dealt with it.

"*That's* what keeps me up at night," Catlett exclaimed:

> When things go wrong, we don't necessarily think of something in the moment, but everything we do or don't do is viewed with 20/20 hindsight. So we find one small issue, and we think we've quarantined it and dealt with it and we can close that book. Well, what happens if it's just the tip of the iceberg, and we should have followed up? Now the Board hasn't fulfilled its duty to look into that issue and mitigate that risk.

"Part of the Target lesson was that it's both the incident response and the way in which you deal with the public relations perspective," Golodner agreed. "It's like the old story in politics: It's not the thing itself that gets you, it's how you react to it. If there's any kind of cover-up, that will *always* get you."

"That's why every other week we brainstorm the questions a lawyer might ask us about what we're doing to protect our assets," Smyth concluded.

The Jewels in the Crown

"The realization of 'When, not if' seems pretty fundamental to changing how we think about security," moderator Johnson suggested to the group. "We're often afraid to call something we're doing in security 'innovative' or 'successful,' because the 'success' in security is that nothing happened. So did

we do something smart, or did we just get lucky? But even so, what are people doing differently today in light of these changes in the environment?"

Eastman's Sturgill began: "One of the keys to winning this war is a smart, educated user. And we have to learn to trust their judgment once they're educated. That makes a lot of us nervous, because we don't control the thousands of people within our enterprise, but no controls or technology are going to protect us if we have uneducated users. So we are investing tremendously in awareness and education."

"Sometimes I think an educated user is the Holy Grail," Smyth agreed, "But how do we protect against users that are not educated, and never will be? We've spent a lot of money on awareness campaigns, on testing the user community, and we have found that there's no improvement, no matter how much we invest. And yet technology continues to develop."

Oliver seconded Smyth's concerns:

> When you take operators who have spent their entire lives in one business model, and that model is now completely changed, it's not always obvious to them when and where new risks are being introduced. So how do you educate them along the way by supporting them, without being viewed as the blocker who's slowing things down, or getting in the way, who's putting undue barriers in the way of success?

"Certain of these measures are not earthshattering," Sturgill responded.

> We do ethical phishing, for example, and we've tracked the success rates. It's been amazingly effective, and it translates not just to the work environment, but also for safer at-home computing. The click rate started in the 30 percent range, and it's now into single digits in our user population. But, we are seeing dramatic increases in sophistication of phishing attacks right now. Spear-phishing, impersonating C-levels is a big concern. If you back up two years, phishing was pretty easy to spot. Not so much anymore.
>
> The next step is to educate users so that they use DropBox or OneDrive responsibly, because these systems can have value. But none of us want our 'crown jewel' documents on a publicly-available collaboration site.

"Say more about identifying and protecting your crown jewels?" Zierhoffer asked. "There's a bigger risk than losing information," Sturgill replied, "And it's the risk that we're not innovative. It's the risk that we're not growing."

> We have to strike this balance appropriately. If I look at all the content in Eastman, I don't care how people collaborate on 90 per cent of it; DropBox is just fine. It's that last 10 per cent that I need to be able to identify and take special and extra care. If we lose this IP, we lose who we are as a company.
>
> There is a very rigorous process to identify what qualifies as a trade secret. When something is classified that way, it has a specific named steward who is responsible for approving who gets

> access to the information around that trade secret, and then it all goes through an annual audit and review process. Ratchet *that* up by 10x, and that's what we do when something is classified as a "crown jewel."

"You still have to depend on the users to do that initial classification to a certain degree," Brooks pointed out. "What is that 10 percent, and where is it before it gets classified as such?"

"We share the nightmare of people using DropBox without thinking about whether the information they're sharing is in the 90 percent or if it's one of the crown jewels," Tenaris' Diaz said. "We've just started addressing this problem. It's a huge challenge in cultural change."

"The interchange of information between Research & Development and Manufacturing and Marketing is always a tough issue," added Carlos Pappier, Tenaris' CIO. "We are in the middle of a big information classification effort — what's Confidential, what's Private, what's Public — and it's a nightmare, because employees are not used to it."

Bechtel's Zierhoffer pointed out a critical problem with the data classification approach:

> Now that the delusion that we can build the walls higher and wider is gone, we rely on classification, which in turn relies on employee education. But all you need is 10 percent of the population to not classify things correctly, or to break the rules, and then you've got a breach. Even if you've got the right policy and practice to identify and protect the crown jewels, you know that the adversary is sitting next to you, not outside your wall, and you can't keep them out.

"We keep a separate SharePoint farm with extra levels of auditing," Eastman's Looney responded. "If anyone touches something there who doesn't normally touch it, we know."

Cultivating a Healthy Distrust

Johnson returned to phishing: "Smart spear phishing looks like it came from an internal box. It passes every filter, gets delivered to the desktop, and looks as authentic as anything internal, other than some odd clues about why you're asking for this now — the timing is a little off. But do you really want to create so much distrust in an organization that people won't respond to internal emails?"

"We want to create a healthy distrust," answered Sturgill. "We do things like dropping USB keys in parking lots. The first time we did it, 11 of 12 found their way to our network; the 12th got run over by a car. But when we do these same things today, it's rare that they make it to the network. Awareness of these issues is at an all-time high in our company."

"This kind of education is an important investment," Smyth added. "Raising awareness and protecting the human is step one in

Tools to Try

A selection of security technologies mentioned by the Roundtable

BitLocker – Drive encryption
Bromium – Endpoint security
Chertoff Group – Risk management
FireEye – Malware protection
Mandiant – Incident response & forensic solutions
RSA ECAT – Malware detection & response

defending yourself. But even if you get the response rate from 50 percent down to 10 percent, it's still too many employees that are going to click on a link."

The Roundtable described other measures being taken to improve security, including federated SaaS identities, single sign-ons, strong authentication models, encryption in the cloud, and data lifecycle and classification. Bechtel's CISO Jose Hernandez pointed out, though, that technology won't be enough if the culture isn't supportive: "Your ways of 20 years aren't going to take you for the next 100 years. We need to be changing."

"The culture of 'Don't change the way I've been doing this for 20 years' is just so strong," his colleague Zierhoffer continued.

> We have to root our way through it, even though it's a business issue, not an IT issue. Security strategy has been around a threat-based defense, and it needs to shift to a risk-based defense. We've begun to use an Active Risk Manager, that the company already used but IT didn't. Now we can say to an executive, "Mr. CEO or CFO or VP of HR, here are all the risks. Here's what could go wrong because of them. You've got to accept these risks." And now *they're* saying, "Oh no, no, no, no, wait!" So it's a good funding mechanism, if you get to that conversation. It's a very different conversation than "You cost too much," or "I don't want you to change my processes."

"We've got to move to this model," Brooks agreed. "We're not making these decisions, and we're not trying to justify our budget. We're just presenting the problem, and asking the business, 'OK, do you want to fund this, or do you want to accept the risks? Your decision; we're just here to help.'"

"Exactly!" Zierhoffer exclaimed. "It's not I who accepts that risk. It's not my infrastructure director, who doesn't have the budget to do something about it. It's *you*."

"Is it fair to say that organizations have moved from a 'Deter' approach to more of a mantra of "Deter, Detect, Respond, Remediate?" Brechbühl asked.

"Everything we do has to fit that mantra. If it doesn't, we don't do it," Hernandez answered. "But the shift to risk-based is next," Zierhoffer emphasized.

Golodner asked what the group thought of the NIST cybersecurity framework, and whether it would be helpful in communicating with businesses and boards.

"Well, it's risk-based," replied Allen. "That makes a lot of sense, and the categories are good: Identify, protect, detect, respond, recover. It's a good nomenclature for risk principles."

"But it won't help with boards per se unless you go through and build out a scorecard to help communicate," Brooks added.

"Communication is the real challenge, isn't it?" Sturgill asked. "The risk is about likelihood and impact. In the cyber world, how do you do that? If we lose our crown jewels, we may not be a company in 10 years. So the impact is huge. What is the likelihood? I can't put a number on that."

"But it's not really your job, is it?" rebutted Allen. "It's your job to consult to the business, to have *them* weigh in, and have *them* put a percentage on it. We're really consultants: We guide the business through security risk management. And in order for us to be effective, we need transparency, and we need independence."

"So that forces assumptions to be made very publicly and very clearly," Brechbühl suggested. "It's no longer somebody doing a presentation, or a technologist sitting in a closet estimating odds. It brings these topics to the forefront, so that there are real discussions, and makes clear that everybody needs to share in the decisions."

"You hit on it," Brooks answered. "First you look and see how your business manages risk today, outside of IT and security."

> And then you figure out how to take IT and security issues and embed them into the same approach. That helps bridge the gap, because the biggest challenge we've always had is to communicate the risks to the business in a way that business people understand it. We had the period of time when it was all fear, uncertainty and doubt, and waving of arms and flaming of hair. Now we're moving towards an actual discussion of risks and repercussions.
>
> I'm a technologist. I know security. I have some business understanding. But I'm not the C-level individual: "You guys tell me: Is this risk acceptable? Or isn't it?"

"My business has a legitimate expectation, though," Sturgill pointed out, "For me as the CIO to come with specific recommendations on which risks we will mitigate. They certainly have veto rights, but I don't want to give that up. It's part of being a C-level executive. The CIO should have the best judgment in this space, because we see the business end-to-end."

"But some of the risk may not be your risk," Allen argued. "You're making recommendations, but ultimately all the risk owners have to be involved in that decision-making."

"I don't disagree," Sturgill replied, "But if something goes wrong, I know whom our CEO is going to call!"

Darwin in the Workplace

Johnson asked each of the companies present to describe their security organizations and information security governance procedures, given all the changes in the cybersecurity landscape. A frequent starting point in the descriptions was how poorly-adapted security organizations were even just two or three years ago. Comments such as "we had little to no information security focus or organization," "our organization was a disaster," and "there was no head of security, and things weren't coordinated at all" resonated through the room, along with anecdotes of intrusions and other security risks and lapses. Fortunately, success stories from changes in organizational, policy, and personnel change were just as common: Cost containment, increased SOX compliance, improved efficiencies, and reduced numbers of incidents.

While each of the six organizational structures presented differed from the others in substantial ways, several common themes emerged:

- A shift in how security risk is managed and perceived, i.e., Zierhoffer's earlier comment on "threat-based to risk-based."
- Closer collaboration between IT and the businesses on cybersecurity.
- Significant increases in personnel dedicated to IT security, along with increased visibility in the org chart for those groups.
- The creation of independent and high-level entities for operations, governance, and rapid response, including Security Operations Centers ("SOCs"), Incident Response Teams ("IRTs"), and Security Advisory Groups, often reporting to the Board of Directors.

TWC's Allen summarized some of the issues that any security organization has to address:

> Security needs transparency and independence, but it's got to be done right. From a transparency perspective, the process is about making sure that all the business risk owners are weighing in and communicating. Security also needs independence and authorization to be able to escalate when needed, and have the ability to do so. If they don't have that capability, then it's ineffective security. At times, there's an inherent conflict. That's not a bad thing: This is the evolution of security practice. Operational separation is necessary for good security practice.

Allen's colleague Brooks described how this approach has played out at TWC:

> We're doing a lot of process changes. Our risk management conversation is more consultative. We're getting in and trying to help the business, to find problems in the beginning of projects so that there's no retrofitting at the end. It's having a significant impact, more so than standing up any new technology.

Diaz described a similar approach at Tenaris:

> We didn't start from a tools perspective, but from a process perspective. We found things that the business owners thought were pretty safe, but were in fact full of holes that could be mended just by changing the process, or making small changes in an application. We picked low-hanging fruit to pilot, and we learned. The first step was to change the consciousness of the risks involved, from the top management down.

Oliver emphasized the change in perception of top management: "Attention level to security is at an all-time high, so we finally have a forum for these types of discussions. Security is now a key contributor to the business, and no longer viewed as coming in to say — again! — that the sky is falling. We're more in business discussions, rather than just raising the level of fear and uncertainty."

"The big change *is* in the awareness of senior management," Pappier agreed. "A year ago, the issue was second priority. Today, it's very high on the agenda."

Johnson asked how the security mandate at the core of the new organizational models is reflected across companies, rather than just within IT.

"In our organization it manifests itself through the audit committee," Coca-Cola's Smyth responded.

> Our CIO is a member, and lot of the initial discussion was around roles and role definition, SOX issues. But the more cyber attacks were in the news, the more the conversations changed to focus on, 'What are our risks as an organization, and what are we doing to mitigate them?' Our CEO is part of that discussion, and our CIO reports directly to the CEO. So it's become a regular conversation at the C-level — no further convincing required. And they've become much better consumers of the information we bring them.

"The things in the media are certainly tailwinds," Sturgill agreed, "And a near-miss will get your attention like nothing else will, especially at senior levels. When we first started down this path, it was 'Oh, no, here's that paranoid CIO again.' Now, it's 'Oh my gosh, what do we need to do?' And the more we communicate what we're seeing to the senior levels of the company, the more buy-in we have for what we need to do."

Brechbühl referred to a finding from a previous CDS CISO workshop: "There were a number of CISOs who were hiring marketing/communications types to help them translate what they were doing to non-technical parts of the business. That's how important the CISOs thought the communications were."[8]

"If We Can Find It, We Hire It"

The conversation turned from organization to talent. "Empirically there's been a shift in the CIOs in the top companies," CDS' Taylor said. "Part of it's because CIOs get the blame, but it's also because the skills needed to be a CIO in a major company are different than they were five years ago. These things go in waves, but right now the turnover in the jobs seems to be faster than it was."

Johnson extended the idea to include the entire organization: "It's such a struggle to find the right talent in this space. What talent do you see needed on the horizon, and how do you see that coming about?"

"Cybersecurity. Data science. If we can find it we hire it," Sturgill said emphatically. "It *is* very difficult. So we're also taking talented, gifted, technically-oriented people with business acumen, and trying to grow them over a period of years: People who are fast learners and are naturally curious about solving complex problems. I would rather hire these skillsets, but we have difficulty locating and attracting them."

"And retaining," Zierhoffer added. "Because they're such hot skills. We train them for a couple of years, and then they just want to go."

---

[8] Center for Digital Strategies, *Information Security Organization and Governance: An Executive Workshop for European CISOs*. July 2013. http://digitalstrategies.tuck.dartmouth.edu/programs/ciso-detail/security-organization-and governance-what-works-in-todays-changed-environment

"We call it 'the two-year itch,'" said Hernandez. "It's not that hard to find incident responders, but when you talk about Information Security 101, generalists who know a bit of everything, it's very hard. We get very good people in one area who know nothing about the other areas, or have no business acumen. I know it can be done; they're just really hard to find."

Brechbühl summarized the various skills criteria for hires in today's cybersecurity organization: "Some business process understanding. Communications skills. Modeling. Analytics. Cyber experience and cyber training. Forensic and investigative skills."

Smyth added to the list: "They have to have a really strong engineering background, with understanding of all the layers of the architecture. Not just applications, not just networks, not just hardware or operating systems. Somebody who has a passion for security."

"So breadth *and* depth of IT skills," Brechbühl amended. "But forensic and investigative skills, or modeling and analytics, are not skills I would have described as traditional IT."

"The forensics come in when individuals with architectural mindsets dive deeper into how the file system actually works, what the artifacts actually mean, how to reverse-engineer malware," Brooks explained. "On the flip side, investigators are capable of understanding the technology, but inquisitive enough to start working their way through how something happened — reverse-engineering the *attack*."

"One of the real challenges," Oliver said, "is how to build a career path for these individuals. Getting them in is one thing, but we're a restaurant company, we're not a technology company. We need those skillsets, but where do we evolve them to? So we're really trying to balance the need for development versus outsourcing, and getting creative with as-needed help."

At Bechtel, Hernandez explained, "On paper the CyberSecurity Incident Response Team ("CSIRT") and the Security Operations Center ("SOC") seem silo'ed, but if you look at their work processes, one depends on the other. The CSIRT is more knowledgeable. So we have a program to graduate people from the SOC to the CSIRT. It's worked out well."

"We have created a lifecycle model," said Brooks. "I *expect* the high skillset is going to leave within a couple of years, so my goal is that by then I'll have someone waiting. We're taking the concept of executive succession planning, and applying it through the entire chain."

Never Waste a Good Crisis

The Roundtable concluded with sobering observations that challenges in cybersecurity are not getting any easier, and hence the requirement for senior-level attention and awareness will only increase.

"I thought we would be alone in thinking that breaches were unavoidable," began Pappier from Tenaris, "But I see that it's the sad reality that we all have to deal with, and that we have to focus on protecting the most important data."

Diaz emphasized Pappier's observation: "The technology is changing every day, and we have to manage both the traditional aspects and the new challenges. So how do we do that? We have to invest in awareness, in involving C-levels and keeping them informed, and making them owners of their own risks."

"We've learned that we can't protect everything," YUM!'s Roush lamented. "All data and all assets are not equal, and so we're not going to protect everything equally. It's validation to move to a risk-based approach, rather than just check-box security. We have to focus on the most important risks to the most important assets."

"That drives home the importance of 'real' security," Golodner added. "Not that anyone's doing fake security, but focusing on those 'crown jewels,' on those things of greatest value, and building out from those core data assets — that's a good principle."

"The governance issue also rises to the top," he continued. "It deals with people, it deals with other organizations that may be stove-piped, and when a crisis is happening, it's too late to figure out the governance. Getting ahead of those governance models beforehand, and then exercising them, is critical. We're finally at the level where Audit committees and Boards of Directors are spending real time on this security, and that wasn't always the case."

"We all have a lot of similar challenges," TWC's Brian Allen continued. "Security is often misunderstood — what we actually do from day-to-day — and so awareness with our employees is a big challenge. What works for some may not work for others, and if it doesn't work, it may be the wrong practice. But keep at it."

"But we can't tag everything as 'security,'" Zierhoffer pointed out. "They get security fatigue, and we're not believed anymore. You can't use that lever every time to get funding. So it's important never to waste a good crisis for your security awareness."

CDS' Taylor summarized by looking towards the next stage of cybersecurity development:

> The 'when not if' idea creates a whole new level of exposure. So much of this job depends on things you don't control — employees, people outside of your organizations, social media. On top of that, the industry is going through fundamental disruption: Everything that affects the skills needed in your roles and your impact on your organizations is fundamentally changing over the next few years. It's going to be a fascinating transformation.

Participant List

Rethinking Cyber/Information Security
June 10, 2014

Brian Allen	Chief Security Officer Time Warner Cable
Hans Brechbühl	Executive Director Center for Digital Strategies Tuck School of Business, Dartmouth College
Prentis Brooks	Director, Information Security Time Warner Cable
Scott Catlett	VP & Associate General Counsel YUM! Brands, Inc.
Gustavo A. Díaz	Information Security Director Tenaris
Adam M. Golodner	Partner Kaye Scholer LLP
José J. Hernández	CISO Bechtel Global Corporation
M. Eric Johnson (moderator)	Ralph Owen Dean and Bruce D. Henderson Professor of Strategy Owen Graduate School of Management Vanderbilt University
Matt Looney	Director, Data Science & Enterprise Architecture Eastman Chemical Company
Charles R. (Dickie) Oliver	VP, Global IT YUM! Brands, Inc.
Carlos Pappier	CIO Tenaris
Melanie Roush	Senior Manager, Global IT Risk and Compliance YUM! Brands, Inc.

Siobhan M. Smyth	VP, Information Technology Leadership Coca-Cola Enterprises, Inc.
Keith R. Sturgill	VP and CIO, Information Technology and Corporate Six Sigma Eastman Chemical Company
Alva H. Taylor	Associate Professor of Business Administration Faculty Director Center for Digital Strategies Tuck School of Business, Dartmouth College
Carol J. Zierhoffer	Principal VP & CIO Bechtel Global Corporation