Center for
Digital Strategies
Tuck at Dartmouth

Information Risk Management in the Digital Age

A Roundtable Overview
Americas Chapter Discussion

Information Risk Management in the Digital Age

Thought Leadership Roundtable on Digital Strategies

An executive roundtable series of the
Center for Digital Strategies at the Tuck School of Business

Information security dominated the headlines throughout 2017, with debate over hacking impact on the US presidential elections and major new data breaches suffered or revealed at Equifax, the Republican National Committee, Yahoo!, Uber, the CIA, and Whole Foods, among many others. By February 20 when the Roundtable on Digital Strategies convened to discuss information risk management, successful cyberattacks had taken place or been revealed in the first 50 days of 2018 at Aetna, AllScripts, Partners Healthcare, FedEx, and the Department of Homeland Security. Facebook's data scandal hit the news two weeks later, and as this overview was in final edits, Delta, Sears, BestBuy, and Kmart announced customer data breaches, all enabled through use of the same third-party website chat technology.

With remarkable timing, the Roundtable gathered at the headquarters of Sysco Corporation in Houston to spend a full day discussing cybersecurity. Topics included changes in the threat landscape, their interactions with developing digital business models, different approaches to enterprise protection, and the evolving role of information security organizations and their relationships to the broader enterprise. Participants included CIOs and information security executives from ARC, the Bank of Queensland, Chevron, Eastman Chemical, Eaton, Elsevier, Sysco, Tenaris, and Tetra Pak, and the Dean of the Owen Graduate School of Management at Vanderbilt University, as well as Executive Fellows and the Directors of the Center for Digital Strategies of the Tuck School of Business at Dartmouth College.

Key Insights Discussed in this Article:

- **Hacking has been commoditized and put in the cloud.** Cyberthreats are increasingly frequent, serious, and existential: Leaked NSA technology, cloud economics, and the participation of wide range of bad actors increase threats, while the digital ecosystem of IoT, cloud apps, and mobile computing increase vulnerabilities, leaving InfoSec caught in the middle**. …. Pages 2-4, 11-12, 15**
- **Basic cyber "hygiene" is still essential, but today's environment also requires high-end SOCs.** Dependable cybersecurity requires a three-part strategy of: (i) expert technical implementation of the basics; (ii) consistent education aimed at increasing awareness of employees, vendors and executives; and (iii) InfoSec analysts and response teams who are as motivated, skilled and innovative as the bad guys. …… **Pages 4, 6-8, 10-12**
- **Overly strict security creates a different risk:** Throttling information exchange and creativity can threaten a company's competitive viability. New infosec roles such as Business Information Security Officers can work with business teams to balance security with innovation and growth. Together they can educate management and Boards — who are often uncomfortably far behind on cyber issues. ……**Pages 5-6, 8, 10, 12-13**
- **The good guys have (finally) started to join forces, too**. As recently as four years ago, most cybersecurity collaboration was on the threat side. As flying solo gets more dangerous, sharing infosec experiences and best practices with supply chains, neighbors (through ISOPs), government agencies, industry competitors (through ISACs), and forums such as this Roundtable is proving critical to minimizing the risk of cyberthreats. …… **Pages 9-10, 14**

© 2018 Glassmeyer/McNamee Center for Digital Strategies, Tuck School of Business at Dartmouth
This overview was written by Stephen Plume, Executive Fellow. The Roundtable on Digital Strategies publication series is edited by Hans Brechbühl, Executive Director, Center for Digital Strategies (www.tuck.dartmouth.edu/digitalstrategies).

2018 Business Model Competition, Cyber Threat Division

The Roundtable last devoted a session to information security in 2014 (*"Rethinking Cyber/ Information Security"*[1]). Hans Brechbühl, Executive Director of the Center for Digital Strategies, launched the discussion by asking the group how the cyber landscape had changed since then.

"The threats are increasing," began Steve Neiers, GM Information Risk Strategy and Management at Chevron. "The biggest change is the speed at which threat actors are moving: Three years ago, it might have been months before a vulnerability was exploited. Now it's days. Three years from now, it will be machine-time, because they're advancing that quickly."

"When WannaCry came out," agreed Bill Blausey, CIO of Eaton Corp., "The vulnerability was announced, and before you could even react to it, there was malware in the world."

"The Struts Jakarta multipart parser exploit probably had the least lead time," added his Eaton colleague Dick Kerr, VP and CISO. "Within hours of its public release, exploits had been packaged and businesses were being attacked in the wild."

Curtis Simpson, Senior Director of Enterprise Security for Sysco Corp., described one cause of the change:

> When the NSA tools were leaked, those were the most sophisticated security tools ever seen. Everyone has been using those: decompiling them, or creating new versions, or just bolting relatively unsophisticated software onto tools that were funded with millions and millions of dollars to target terrorist and criminal organizations.
>
> That changed the game like never before. The attacks have become more sophisticated, and faster as bad actors continue to iterate. They went from WannaCry, which was relatively unsophisticated and just bolted onto NSA tools, to NotPetya, which was a lot more sophisticated, in just 30 days.

Selected Cyber Events, 2017-2018	
Month	**Event**
April 2017	NSA tools leaked
May	WannaCry
June	NotPetya
September	Struts exploit
October	Dyn attack
January 2018	Meltdown, Spectre

"One of the severe threats we're facing is being bystander casualties to nation-state activities," Neiers pointed out. "NotPetya was directed at Ukraine by a nation-state actor, and there was a lot of collateral damage. You don't even have to be targeted: You just have to have a presence in the country, just be on the sideline. How do we protect ourselves when one nation-state goes after another?"

"More of these attacks have been just malicious," observed Rich Licato, CISO for ARC. "They're about targeting a certain company, or service, or nation-state, and destroying it. They're not about data exfiltration or anything like that: The goal is destruction. And if I'm in that path, I risk being destroyed as well."

"It's true that the speed and volume of highly-sophisticated nation-state types of attacks are increasing; it's highly intense," summarized Tim Sarvis, Director, Information Security and Services at Eastman Chemical.

[1] http://digitalstrategies.tuck.dartmouth.edu/programs/rethinking-cyberinformation-security/

> But there's also a level of not-so-sophisticated attacks that can be just as operationally disruptive. The level of investment required for that type of unsophisticated attack is insignificant, even for just two or three people, and yet the gains can be tremendous. So the difficulty is that you have to have capabilities in place to protect against both the sophisticated and the unsophisticated types.

"The nation-states attack their targets just as they would with physical weapons, to take them down," Kerr distinguished between the two motives. "While the criminals are stealing — they want to make as much money as they can."

"The monetizable business model started with ransomware," Simpson recalled, "So now we are also going to become collateral damage in the battle for Bitcoins and other cryptocurrencies."

> With Meltdown and Spectre, in the US we're already seeing a massive amount of compromise by people trying to consume resources to mine Bitcoin. Their next target is to steal information and go after cryptocoins in a big way. In some cases, this will affect entire economies.

John Kelly, Global CISO at Elsevier, explained further:

> Things like the NSA tools got out, and now you don't have to be smart to be a good hacker: Hacking, just like everything else, has been commoditized and put in the cloud. There used to be a relatively small hacker elite, but now you don't have to be smart to be a good hacker. Anyone can go rent these tools that have been weaponized and commercialized in very dangerous ways.
>
> With so many people "just trying it out," the big danger is the growth of the attack surface. As a hacker, you don't need to have great, in-depth technical experience anymore: You just need to be right a few times, when someone has a bad day.

"The accessibility to the tools is just unfathomable," Simpson marveled. "You can download software, install it within five minutes, and with a couple of clicks, you can execute damaging attacks against vulnerable environments. There are sites now where not only can you rent the software, you can rent the *service*, and take a payback from the result!"

"What Does Security Look Like When You Can't Trust Anything?"

Simpson continued to catalogue changes in the threat landscape:

> Not only are the threat actors making more and more money with what they're doing, but they also have new and unique ways of doing it. The Dyn attack was eye-opening: The IoT has been a dark spot for many of us, and it's growing rapidly. Almost every device that comes into an environment now — vending machines, smart safes, everything — is an IoT device.
>
> From a business perspective, we're using the IoT more and more — to be competitive, to do new and unique things we've never done before. But the criminal actors are noticing. The NSA tools were going after the devices that nobody looks at, the devices in our blind spots: the IoT devices. So now we're exposed to attack paradigms that we've never seen before: Botnets that are invisible to all of us, but pounce when the time is right.

"And the more we connect devices to our networks, the more information we are putting into and

sharing in the cloud," added Luis German, Chief Process and Information Officer for Tenaris:

> Whether it's from IT, or from cowboys just hooking things up. We don't even have the data on our servers anymore: It's 'somewhere.' Security is no longer a matter of what we do internally; it's also what's happening in the environment, and with our partners. Sharing information is one of the most complicated challenges we have as we move forward, and we are all being exposed on a daily basis. We now depend on other people doing their jobs for us to be protected.

"The tendency is to believe that security is now somehow the cloud provider's problem," Blausey agreed. "But people spin up new environments all the time, and unless they have it engrained in their brains how to do it in a secure fashion, those environments are exposed."

"Absolutely, we've increased the risk," Kelly emphasized. "The number of vendors we now interact with, the amount of information we share, with almost no visibility into any of the services they're providing. It went nuts when anybody with a credit card could spin up something new with a new hosting provider. What is the level of security from vendors we don't know, who aren't connected to IT?"

Kerr expanded Kelly's point:

> The hardest part is when vendors change status. You brought in a vendor, and they weren't classified as strategic at the time. Over time they became strategic, but you never recognized that, so you never changed your practices, your monitoring, your accountability. The business does this all the time. They'll bring a vendor in with a small footprint, but somebody else is working with the same vendor totally differently, and now you're dealing with a security mess.

"That's why you have to get the business more involved in what you're doing," counseled Dickie Oliver, CIO of ARC.

> You have to get their attention: "Yes, you can spin up a cloud environment on AWS, and fill it with data extracted off your laptops that you've been saving in emails from a third-party ISP, and you can probably use all that to do great things. But now you've also put the whole company at risk."
>
> Then help them understand why you are attempting to do what you're doing, and help them be part of a solution that moves away from the high-risk approach and still makes them more flexible or agile or whatever they want to be.

"The biggest change from everything we've talked about is that there is no perimeter anymore," Simpson concluded. "It's long gone. If something is behind the firewall, that's irrelevant, because we all have our own devices, we're all accessing cloud services from home, from work PCs, from wherever."

"But not all of these changes are just massive challenges that increase exposure levels," he suggested. "They will if we don't manage them effectively, but we also all have data centers with vulnerabilities we'll never be able to address."

"If we look at where we were with our data centers, and everything that we've now outsourced to Amazon, with how much time and effort and energy they put in, I think we're in a vastly better position than when we were running them," confirmed Richard Hebdon, VP of Technology, Infrastructure, and Operations at Elsevier.

"You all shouldn't feel so bad about the progress you've made," advised Eric Johnson, Dean of the Owen Graduate School of Management at Vanderbilt. "I spend most of my time in healthcare, and talk about the wild, wild west:"

> Imagine your factories with customers and vendors and employees all walking around, connecting into control systems or playing with a robot, at any point in time. That's essentially what hospitals are: You have patients, families, outsourced vendors, staff, and a wireless internet of things that has developed organically over time. Take a wireless infusion pump, for example: How many different people could be connecting into that? A bad attack doesn't steal data or take money: It kills people.

"It's completely out of control," Johnson finished. "What does security look like when you can't trust anything?"

No Risk Is the New Risk

"There are bigger risks to the business than information security," suggested Keith Sturgill, CIO of Eastman Chemical. "The biggest risk is that we lock data down to the point where we don't innovate, we don't grow, and we're not competitive anymore."

"The pace of change has increased exponentially," added Mark Meyer, Head of Global Information Management at Tetra Pak. "The pace of development, the pace of staying in business. A competitor may play a bigger risk than you, and they may get the reward. Or they may get wiped out. I don't know the answer, but if you're really risk-averse, and you operate that way, you're risking the business."

"The biggest risk is the risk of the business not moving," agreed Gustavo Diaz, Information Security Director for Tenaris. "We need to understand clearly what the business wants, and never say, 'You cannot do that.' We can say 'Do it this way, or this other way,' but we can't stop them: If we do, the business will step to the side and move on without us."

"There's a constant battle between using digitalization to improve the customer experience and keeping the customer's information safe," illustrated Janelle McGuinness, General Manager, Digital and Innovation for the Bank of Queensland.

> As a bank, we are in the business of trust — that's all we have, really. If the security teams aren't working with the business, the business will find another way: They have targets, they have KPIs, they have to move quickly. If you're too restrictive, it's too easy to find another way, and you won't know until it's too late. Often the security risk isn't the outside attacker: It's just employees trying to find another way.

"And some of this creates opportunities," Simpson asserted.

> People export and share information out of legacy HR systems all the time. They do things that prevent you from locking those data crown jewels in a safe and protecting them effectively. When you move to a solution like Workday, yes, it's all in the cloud, but you have a full toolbox to help the business operate the way they want to. You're helping them be more effective: They can do their jobs more easily than ever, and now you have a crown jewel safe that you can secure like you've never been able to before.

"So, there's a lot going on that's positive for the business," Brechbühl summarized, "But these same factors open us up to more vulnerability. You may have cost savings with the cloud, or it may make you more nimble, but you're also more exposed. How should we be dealing with this very clear tension between the positive aspects of digital business and the difficulty of securing our data?"

"IT has been in the discussions about how to take advantage of new digital capability and new business models for a long time now," Sarvis responded. "Now Information Security needs to get itself embedded in those same conversations. That's the only way to do digitization safely, versus different parts of the company procuring or implementing new technology, and information security turning into an afterthought."

"Whatever it is they're trying to do, 'There's an app for that,'" Hebdon concurred. "We have to realize that we're competing with all kinds of external services. We have to be the path of least resistance to the business, or they're just going to bypass us. We have to be part of those early conversations."

"If we can be there at the first conversation," Diaz finished, "It makes a lot of difference. Then we can understand what the business needs, and how to maneuver solutions for them."

Danger Ahead: Proceed with Caution

Kelly described one element of Elsevier's approach to facilitating conversations between business teams and InfoSec:

> We've created an organizational concept called the Business Information Security Officer, or "BISO." They're direct lines to the application development organizations, and they embed themselves in the project slate for two purposes: One, to ensure that our security tooling and services are present; and secondly, to give us feedback on what's going on inside. We were getting a lot of false positives from some of our tools, and the developers were losing faith in what they were given. So we introduced different tools to the stack, and helped the developers learn how to use them.
>
> The more aware we can get people to be, then the more aligned they are, and the earlier we can get involved in whatever the business is planning.

"The biggest change for Chevron," Neiers offered, "Is that we developed an enterprise risk register for cyber security. For the first time, we're going to be able to understand all the risks across all our different business units."

> We'll be able to focus on our biggest risks, and that will help us focus our spend. It's also helping us do a lot of education with our leaders, and to have the risk dialogue: "Here are your threats, here are your vulnerabilities, here would be the impact. Now, let's have a dialogue about what we need to do as a business."
>
> Finally, we've inserted cyber security into our operational excellence "Bible." That's helping to raise awareness on how we treat cyber risk at Chevron, and to ingrain it in our culture.

Simpson tackled another major source of risk:

> Sysco grows a lot through acquisition, and we've spent a lot of time refining our acquisition model: Knowing the risk of the companies that we're purchasing, and building a model around

that, as opposed to buying a company and later saying, "What, again?!"

> Now when we buy a company, we identify one or two IT people we're going to interact with. We work with them to manage the highest risks upfront, and then understand and prioritize the rest of the risks, and manage them together. There's no appetite for buying a breach.

"A typical acquisition target might be 90 releases behind on Microsoft," explained Simpson's colleague Wayne Shurts, CTO of Sysco. "That's an actual number. So we've become very cautious, and Curtis' team has to give the green light before we even connect networks."

"Eaton has also grown a lot by acquisition," Kerr agreed. "Historically we've done a good job of getting newly-acquired businesses aboard the network safely, of making sure the acquired footprint has been remediated to an acceptable level of security before integrating. Where we've been less diligent is driving foundational security improvements, and we're now putting a lot more emphasis on fundamental hygiene."

"As an aerospace provider we had no choice," Blausey explained. "It was driven by DFARS[2]. All the cyber assessment tools, whether from NIST or any of the others, come down to basic hygiene, and to where we should spend our time to address the greatest risks. They're structured and methodical, and we feel much better about the way we collectively approach things now."

"We use the US-Cert Cyber Resilience Review," ARC's Licato chimed in. "It's a great self-assessment tool with everything in one package. It provides a really nice heat map that tells you where to focus."

SOC It to 'Em

In EY's *20th Global Information Security Survey 2017-2018*[3], 48 percent of the nearly 1200 companies surveyed still didn't have a Security Operations Center ("SOC"), even though "only 4 percent of organizations are confident that they have fully considered the information security implications of their current strategy."

"The companies here are at fairly varied levels in terms of SOCs," Brechbühl observed. "They're also different in terms of how much is internal vs. external. What have we all learned from these efforts? What have you done right or wish that you'd done it another way?"

"At Eaton, we were very thin internally and not able to fully leverage the tools and capabilities we had already purchased," Kerr answered.

> So we took our SOC to a third party, and worked extensively with them to get detection and correlation in place at the levels we wanted. That's enabled us to build our internal staff, focus on level two and level three activities, and do threat intelligence and hunting that we didn't have time for before. It also gave us 24x7 coverage, which has become a necessity for rapid response. Now we're outgrowing our SOC provider's capability to keep up, so we'll be looking for next-generation capabilities, including how to integrate faster with cloud-based and third-party services.

[2] Defense Federal Acquisition Regulation Supplement

[3] http://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf

"We outsourced as well," recounted Robert McIntyre, Director of Information Security for Tetra Pak, "But we found that the vendor could never understand our environment as well as we did. They couldn't scale to what we needed in the technology, and we spent more time talking with them about what we do than actually analyzing any of the data. So, we wound up bringing everything back in."

"The biggest advantage to an insourced SOC is that they can provide business context to what they're seeing from threat indicators," Sarvis proposed.

> It's difficult to think that we could get a third party to the same level of business context that we'd want to see within a SOC. We do have a lot of automation in place, but there are certain aspects where people are the first line of defense: You want them to understand exactly why the sirens are going off, and how they should respond to that level of alert. Do they need to roll the fire trucks, or is just a bunch of false alarms? This business context is critical when you're looking at threat indications against your enterprise.

"We share all those same concerns, but we also know that we can't staff sufficiently," Simpson countered.

> To balance those risks, we've worked with our provider to have their team leads be part of all our services. They're embedded in our ops teams: They hear the risks we talk about, what's working, what's not working. They hear what Engineering has built into the landscape.
>
> Historically there's been a wall between these two teams. Now they're in the same room, every day. They've become one team, and a lot of the problems have dissipated, because they're all talking about the business challenges and the new technologies. This has been a game-changer for us in terms of making the service more effective.

Neiers gave an example of how Chevron's SOC made a material difference:

> Our SOC data identified that phishing e-mails were our biggest intrusion vector, so we made a concerted effort to strip that down. First we put an "external" tag that helped people identify messages that might have a little more risk. Then we put in some technology to strip out any emails with malware in the attachments, and implemented the "Report Spam & Phishing" tool in Outlook.
>
> Finally, we used an external company to develop phishing tests. We set a goal of half the industry average hit rate, and we put in an accountability model: Fail once and take a training; fail twice, have a HR-record discussion. Our average click-rate is now 10 to 20 percent of the industry average. Most importantly, actual phishing incidents moved from 30 to 40 percent of our overall incidents to now 0 or 1 phishing incident a month.
>
> An increasing problem is related to our third-party vendors. In 2016 we had a handful of phishing attacks from legitimate email addresses at legitimate companies who had been compromised. Last year, we had 35 times as many. We've caught most of those because we have built enough awareness, and people now get suspicious about "Why is Joe sending me an invoice? He never sent me an invoice before…."

German described a variation on the vendor phishing scheme: "Attacks are not happening towards us, but towards our vendors in relation to us. They get an email, that looks like an official Tenaris email, that says, 'Please pay us through this other bank, instead of the one we've been using.'"

"Vendors getting compromised is one of the biggest threats we have," McIntyre admitted. "A legitimate contact with a legitimate supplier tries to re-direct payment. We've had to put in a business process that ensures payment details cannot be changed through an email."

"And of course a supplier's initial reaction is, 'No, our systems are not compromised, we don't have a problem,'" Kerr sighed. "It often takes days of showing them 'Here's what we received from you' to get them to 'Oh crap, we've been compromised.'"

"We used to see that a lot, but it's really fallen off in the last two years," Blausey demurred. "There's more awareness that this is a typical scenario, and that anyone can be compromised. So we see less resistance to making IT-IT or leadership-to-leadership connections, and having the dialogue of 'There's an issue here, let's work together to resolve it.'"

"The size of the players is the issue," pointed out Twila Day, Managing Director at Alvarez & Marshall.

> Your companies are larger, and you can afford to put a lot of things in place. But those mid-tier and lower-tier companies don't have the same sophistication that you do, and it's very much harder for them to be able to address these issues. How much you take on, and how much you try to enable them is the key, because they don't have the staff or money to be able to do a lot of it.

"A lot of it boils down to setting the rules at the business process layer, as opposed to just awareness," Sarvis suggested. "With the human element in the mix, you're never going to get it 100 percent right. If you see an invoice coming through a method that your business process is completely against, there should be automation to flag it, instead of having a human remember 'Oh, yeah, this must be what I was educated on.' Embedding rules in your business process stack is the only way to really solve the problem."

No Easy Answers

"What are you doing to protect the data itself?" Brechbühl asked. "Is that a strategy that's successful, or cost-prohibitive? Does it hamper business processes?"

"A lot of our valuable information is unstructured, and so it's not in the ERP system," Diaz answered. "It's in SharePoint or somewhere, in the form of a machine plan. We used to have no controls whatsoever, but now we've implemented a digital rights management system that's very good. It controls access, and sends access alerts, even for the people who have the proper rights."

"Information classification is going to be our success story once we get through the growing pains," Meyer volunteered. "All information has to be classified. We've built this into Office templates, and enforced it in the ERP and other systems. You can't create or save a document without selecting what the classification is."

"There are business implications of that," he acknowledged. "If you classify something as Restricted, then immediately a set of rules apply, and someone complains that we're getting in the way of the business. But once you figure out what your pattern should be, it's not that intrusive. It's only intrusive when you misclassify or misuse."

"We've done the same," Diaz' colleague German declared.

> The learning curve does improve with time, and we designed it so each organization on the business side can decide for themselves what rules apply to their data. So when we get a complaint, we show them their own definitions: "IT isn't imposing anything on you. This is your classification; change it if you want to." We put the trade-off decision on how complicated it gets vs. how much protection they want onto the business.

Meyer extended the scenario: "Once the culture of classification is in place, maybe everything doesn't have to be classified, maybe it's only a certain group of things, and everything else can receive a minimum level of attention. That helps with the cost and the impact, and focuses attention on the special stuff, on the crown jewels, where you do need to invest more."

"It's complicated," Sarvis observed.

> You might have a CFO who wants to lock down the financials, but an innovation group that is trying to do something unique to create new opportunities. It really gets down to your version of "confidential:" If it's internal, should everybody get to see it, so they can be innovative? It's not technology that's the problem; it's getting in sync on how innovative we are going to allow our people to be. There's no easy answer to this.

Sturgill's response echoed his earlier comment on the risk of restricting innovation:

> We have a hard-core engineering culture, with a lot of black and white thinking. In the past we've asked, "Could this information possibly be used to harm us?" If the answer was "Yes," then we locked it down. Now we're moving to black and white with a broad area of gray: "Yes, in certain cases it could harm us, but how likely is that versus the rewards we'll get from having a more open look?"

"You can't know how innovative something might be until you see the data and the connections, so how do you open things up enough to actually be able to look for an innovation?" McGuinness asked.

> Back to the balance question: If things are automatically classified, then you don't know what you don't know, and you've already ruled yourself out of that potential discovery. Should we assume that everyone is evil? That's what we would do naturally from a security standpoint, so "Lock it down!" Or in this new world of things moving so fast, should we assume that things are OK, until they're not?

"The globalization and digitization of business is making all of this change," Day agreed. "The conversation really needs to be around asking if there's a reason something won't work, instead of pushing the business to prove why it will work."

"But if you err towards openness, the insider threat becomes much more real," Sturgill objected. "Not the fired salesperson who downloads your customer list, but someone who's in your organization with the sole purpose of stealing your intellectual property. They're authorized to do what they're doing, and you have to detect when they're doing it in a way that looks malicious."

"That's why there's not one answer to this problem," Simpson responded.

> If you do want a more open culture, then you have to monitor behavior around how data is being used. Certain things get assigned from a role-based perspective, and if you need to know, you get access. For everything else: I don't care unless you tell me I should care. Then if there

> are behavior deviations, you're going to want to respond. Behavior analytics is new for us, but we're diving in deeper, because I don't know that there's a better solution.

Shurts summarized the challenge: "There's value in not letting the bad guys get hold of our data. What we have to navigate is, there's tremendous value in letting our people get hold of our data to make better business decisions. You have to weigh them both, and you don't want to shut the latter down because of the former."

"And let's be clear," Simpson finished. "This isn't 'Who can I persecute today?' What we're looking for is malicious behavior, and it will raise its hand at you every once in a while. I don't want to use the tools for persecution; I want to use them to manage risk in the environment. And as insider risk becomes more prevalent, we're going to see greater linkage between physical security and information security."

"You're looking for what Phil Venables at Goldman called 'toxic combinations,' Johnson observed. "Someone looked over here, and then he looked over here at something he doesn't usually have access to, and putting those two things together sets off flashing red lights."

"Breaking down the siloes is really important," warned Alva Taylor, Faculty Director of the Center for Digital Strategies.

> Triangulating data and communications and personnel records, to find bad things together, or to see patterns that don't seem to be natural patterns. Then you don't approach the person and say, "We're calling you in because you're doing something bad." Instead, you say, "We're worried that someone has your account, we're worried for your protection. Help us understand why these things might occur in this way."

#ForTheBoard

"Universally you describe awareness as up among the population of your companies," Brechbühl observed. "What you want is for everyone to be a defender of the faith, but that doesn't necessarily happen. How do you get real, true engagement?"

"Education and awareness are critical," Sarvis answered.

> We are a manufacturing company, and you can speak to any employee, to any contractor, about safety, and they know the tagline, they know there are consequences if they don't act in a safe manner. The same is going to have to be true from a security perspective, and fortunately or unfortunately, it's going to help spread awareness that there are a whole lot of things to focus on.

Sturgill described one of Eastman's awareness practices:

> Tim's group produces a newsletter based on the idea that if we can help people be safer in their computing practices at home, they will have a better awareness and will do a better job of protecting information assets at work. It's not in the super-sexy category, but it is effective.

"Another thing that's helping is the level of passion brought by the new recruits coming out of university," Sarvis added. "They've grown up understanding cyber, and they've done hackathons, even in high school. There's a huge difference now between an applications analyst and a security analyst.

When our executives visit the SOC and talk with the analysts, their comment is 'Those people take it personally. They're trying to protect the company like they're trying to protect their own homes.'"

"On the one hand it's good that there's this new awareness at the executive level," Meyer countered, "But the other side is that suddenly management and boardrooms are talking about things they have no clue about. They are putting on pressure, and dictating responses on how we should actually do our jobs that make it much more difficult to address all this complexity."

"We're constantly going into the conversation underwater in trying to bring the Board to the level of what we're about to do, or attempting to do, or proposing to do," Oliver agreed.

> There's nothing we do today that's not technology-enabled, and these are multi-million-dollar decisions that we're trying to get these folks to align on. So it's critical for us to continue to chip away at building partnerships with the business. We need to say to them, "Don't tell me how to provide xyz environment; tell me what you want to do. Then let's work together on the best way to deliver it."
>
> This conversation has to go all the way up to the boardroom, articulating a story that makes sense to a bunch of board members who move in and out of your organization once every four months: "Are we secure, are we going to have an issue?"

"It's a small trick, but can you tell your story without using an acronym?" Taylor asked. "You have to be able to, in order to get it to translate. And even if you have to explain later, it's a good litmus test."

Day emphasized Taylor's point: "That ability is a key skill set: to take something that is technical by nature, and to formulate the policies and the awareness programs and communicate them back to the business, without it just being a scare tactic."

"For one recent board presentation I had the COO deliver part of it, and the chief HR officer deliver another part, because I wanted to communicate that what we're doing is critical to the entire company," Oliver reflected. "What they described wasn't technical in nature; it was how the work we were doing in technology was impacting organizational change. Everything we do is in support of the business, and we have to be careful of those presentations that push IT and infosec off to the side. Every company is now a technology company; some just don't know it yet."

"Most boards don't have technology experience," Simpson agreed. "When you walk into that room, you'd love to be able to say, 'Here's where we are now; here's where we need to be; here are the challenges we're having.' But the problem is you have to take 10 steps back, and educate on the foundation, and then get back to the conversation, and no one wants to talk that long."

"Our recent breath of fresh air is that a technologist has joined our board," he continued. "Her experience and her passion around what we do enable her to challenge us and the board in the right ways. This is going to be a big win for us. Every board needs a technologist on it, because otherwise we're going to face this challenge until the end of time."

Burning Down the House

"With all these different aspects to it, does information security ever become a competitive advantage?" asked Sravya Yeleswarapu, a second-year MBA student at the Tuck School. "Or should all companies in

your competitive landscape be at the same level, because they're dealing with industry-wide issues?"

"Today it's not a competitive advantage," Meyer answered, "But as we move into plant automation, *everybody* has the problem. If we put security at a level that our competitors can't, that could be a competitive advantage for us."

"For us, it's not a competitive advantage: Our 'competition' is the threat actors," Neiers said. "For third-party vendors, though, if they're risky, then I'm not going to use them. So it could be a competitive advantage for that kind of company, if they're doing things correctly."

"Security may not necessarily be a competitive advantage," German countered, "So much as just a necessary element."

> Transunion may have gained customers because of the Equifax breach, but probably more as a disadvantage for Equifax than an advantage for Transunion. I don't think security is an element that we'll intentionally use to compete. It's a common threat beyond the strategy of individual companies.

"This type of event is damaging to the industry as a whole, to the entire market segment," Hebdon stressed.

"No one can fight this by themselves," McGuinness warned. "No one laughs at anyone else when they get hit, because that could just as easily be you. It's a collective effort to try and stop it. Even though the financial services industry tends to be quite confidential about most things, it's probably among the best at sharing data when it comes to threats."

Blausey pointed out an important exception to sharing among participants in the same industry:

> We collaborate with many organizations on information security programs, but I don't see that happening on the product side. That's a whole different game: I can't fathom working with a competitor on security issues that are built into our products.

"We are starting to invest in information exchange as well," Sturgill affirmed. "We participate in groups that are trying to bring the industry along, and we are helping form a chemical industry ISAC."

"ISACs are great," Neiers agreed. "We started an oil and natural gas ISAC three years ago, with 9 companies, and now we're over 40 members. It creates a forum for frank conversation about what we're each doing well and not doing well, and how we can help each other. I can't say enough about the ability to share information: It makes a big difference in what we're doing. And to add to this point: Get to know your local FBI."

"And I'd add to all of those the concept of a regional, cross-industry ISAO," Kerr proposed. "It's a different animal than an ISAC. It's been both interesting and valuable to have a cross-industry perspective of shared threats. We have seen many more attacks that touch multiple members across manufacturing, energy, education, banking and finance than I would have thought."

"Maybe this group of CISOs should stay connected and keep a dialogue going," Shurts proposed. "Our discussion today reinforced some ideas and introduced new ones that we can take back to our workplaces. There's value in connecting with different groups in your city and your industry, but there would also be a tremendous amount to be learned by continuing to share with the CISOs in the room."

“Even for companies that think they have a competitive edge on security, it’s a bit like facing a forest fire,” Johnson suggested. “You may think you built a good house all by yourself, but when the fire comes, maybe you don’t really know. You’d have to be really confident to live alone.”

“Confidence in this space can be very dangerous,” Shurts cautioned, “And security can become a massive competitive *dis*advantage.”

> But it’s also easy to get lost in the big heaviness of all this. The best way to stay safe is still really good blocking and tackling. Go back to Petya, WannaCry, and all those things: If you’ve done the basics well, you can stay safe. Not that the basics will keep us safe forever! But they’re probably still the most impactful things to focus on.

“Sometimes we do get seduced by the sexiest exploit on *World News Tonight*,” Kelly confessed.

> So most investment has been in sexy new tools: “If I invest a lot of money in this tool, then I'll be protected from this attack.” But in reality, we see time and time again, the fact that you have the tools doesn't negate the fact that a lot of the companies aren't using them effectively or completely, or the penetration of the toolset is not fully deployed from where it needs to be.

“At the end of the day,” Kelly finished, “Being good at basic hygiene is 80 percent of being good at protection.”

Participant List

Information Risk Management in the Digital Age
February 20, 2018

Bill Blausey	SVP & CIO Eaton
Hans Brechbühl *(moderator)*	Executive Director, Center for Digital Strategies Adjunct Professor of Business Administration Tuck School of Business, Dartmouth College
Twila Day	Managing Director Alvarez & Marsal Executive Fellow, Center for Digital Strategies Tuck School of Business, Dartmouth College
Gustavo Díaz	Information Security Director Tenaris
Luis German	Chief Process & Information Officer Tenaris
Richard Hebdon	VP Technology, Infrastructure and Operations Elsevier
M. Eric Johnson	Dean Owen Graduate School of Management Vanderbilt University
John Kelly	SVP & Global CISO Elsevier
Dick Kerr	VP, Enterprise Architecture Eaton
Rich Licato	CISO Airlines Reporting Corporation (ARC)
Janelle McGuinness	General Manager, Digital and Innovation Bank of Queensland
Robert McIntyre	Director, Information Security Tetra Pak
Mark Meyer	Head of Global Information Management Tetra Pak

Steve Neiers	GM, Information Risk Strategy & Management Chevron
Dickie Oliver	VP & CIO Airlines Reporting Corporation (ARC)
Tim Sarvis	Director, Information Security and Services Eastman Chemical
Wayne Shurts	EVP & CTO Sysco
Curtis Simpson	Senior Director, Enterprise Security Sysco
Keith Sturgill	VP & CIO Eastman Chemical
Alva Taylor	Faculty Director, Center for Digital Strategies Associate Professor of Business Administration Tuck School of Business, Dartmouth College
Sravya Yeleswarapu T'18 *(observer)*	MBA Fellow, Center for Digital Strategies Tuck School of Business, Dartmouth College