SDA Bocconi
SCHOOL OF MANAGEMENT

Tackling the Cyber Challenge

Key Insights and Summary

Tackling the Cyber Challenge

A Digital Strategies Roundtable
An executive roundtable series of the
SDA Bocconi School of Management at the Università Bocconi

As threat actors become more capable and numerous, it is becoming ever more difficult to protect the systems, people, and information inside our corporations. Digital transformation connects everything, making data ever more central to competition while making operations ever more vulnerable—trends that have only been accelerated by the pandemic. This roundtable focused on info/cyber security strategies to tackle these in both traditional IT and the increasingly important and vulnerable security domain of OT.

CIOs and cyber/information security executives from the American Bureau of Shipping, Airlines Reporting Corporation, Chevron, Conagra Brands, Eaton Corp., Levi Strauss & Co, Nestlé, Owens Corning, Tenaris and Tetra Pak convened at the Houston headquarters of host Huntsman Corporation. They were joined by faculty, students and Executive Fellows of the Digital Strategies Roundtable from the SDA Bocconi School of Management.

Key Insights Discussed in this Article:

"There are only two types of companies: those that have been hacked, and those that will be."
— Robert Mueller, FBI Director, 2012

No Magic Potions

Enterprise digital transformation has become pervasive, and in many ways was accelerated by the COVID-19 pandemic. The variety and sophistication of cybersecurity threats have both increased, as has the cost and severity of successful attacks. In response, IT and information security organizations have been forced to evolve their cybersecurity strategies, with consequent changes to goals, processes, organizational skills, and leadership.

"The attack surface is increasing", explained Robert McIntyre, Director of Information Security for Tetra Pak, "Because everyone needs data, all the time."

> That means legacy products and devices with poor security or poor architecture are being connected in ways they have never been before, including OT equipment in production environments. That trend is accelerated by today's speed of business—customers need engineers to deliver new capabilities asap, often without having the time to review or develop appropriate security.
>
> We simply can't protect the forest anymore—we have to protect every tree in the forest, and there are a whole lot of trees. Whether we're looking at our customers or our own OT production environments, data is needed for everything, so you need to connect everything.

"Too many CISOs are told they just have to try to keep up," observed Jonathon Coombes, CISO at Conagra Brands. "Or that security will get bolted on afterwards. Cyber security needs to be built into the entire journey of transformation—the culture of security needs to be paramount from the beginning. The key thing to realize is that the points of control are changing. There's a great post[1] that talks about four key tenets of the new architecture:"

1. Cloud is the new data center.
2. Any device is now a work device.
3. The Internet is the new network.
4. Identity is the new perimeter.

"The whole concept of the perimeter has become diffuse," agreed Gustavo Diaz, Senior Director of Information Security at Tenaris.

[1] Jarrod Benson, https://www.beyondidentity.com/resources/jarrod-benson-ciso-koch-industries-securing-cloud-and-passwordless-identity-management

The long-term shift towards remote working means that users, devices, applications and data are moving outside the enterprise's zone of control, and new business processes driven by digital transformation increase risk.

"Trust but verify" is no longer an option: advanced and targeted threats have moved inside the corporate perimeter, and perimeter-based security is not compatible with today's business models. We managed perimeter defense-in-depth for years, with good results, but in this changing landscape, we are embracing a new approach, 'cyber resilience.' Resilience depends on zero-trust, but there's no magic potion for it.

PRINCIPLES OF ZERO-TRUST & RESILIENCE

- Protection surface instead of attack surface
- Network segmentation
- Least possible privileges
- Strong authentication, for devices as well as people
- Control & visibility

Things That Go Bump in the Night

"Most of what we see is increased risk of threats that already exist," observed Paul Townley, Owens Corning's Vice President of Global Information Security.

> For example, in the past employees in production facilities mostly didn't have access to computers. Now, with advanced process automation on shop floors, they're getting more access, so the risk of insider misuse is going up, and we have to be able to authenticate all the shifts on the production line. Similarly, we've seen an increase in ransomware of suppliers and customers. If we don't hear from a third party for a couple of weeks, we often find that they've been ransomed.
>
> Externally, the main thing is the attack surface. We all know what's behind our firewalls, but as more and more software and services move to the cloud, it gets harder and harder to know where everything is, and what may connect backwards. The big cloud-based automation vendors are high-value targets for the hackers, and we have to figure out ways to mitigate the risk in case something happens to one of them.

"For all these reasons, we've been doing zero-trust for a long time," Townley concluded. "Our data only goes onto devices that we control."

"Remote and hybrid access is also expanding," added Richard Licato, CISO of Airlines Reporting Corporation (ARC). "And we don't want to care how you're coming in. But no matter what you're doing or how you're coming in, we get to monitor and control that experience. If you want to use your own device, go right ahead, but you're going to be limited in terms of what you can do and what you can see. If you use a managed device, we'll open the world to you, but we'll still monitor you and challenge you every step of the way."

Adriel Ginsburg, CISO for Huntsman, described yet more developing threats:

> One of the things that keeps us up at night is that hacking-as-a-service has become such a problem. You no longer have to be a genius hacker to break into a company—you just have to have the cash to pay someone to do it. You can contract that service right out in the

open, seven days a week. Attacks are also far more complex. The bad actors don't just bang on the front door anymore: They create fictitious accounts on WhatsApp (which we do not use) that copy people's pictures, copy mannerisms, and they're very targeted against specific employees.

There are also challenges with remote workers. Two years ago everybody went home, but it wasn't too big a problem to connect people and externally-facing systems via VPN. But when people work at home for a year, and the patch management process requires them to sign onto the network every six months—now the corporate devices are a year behind in patching. They're vulnerable, and you don't even see it because you're not scanning them while they're off-network. So you have to develop new patching processes.

Likewise, ransomware has evolved. We are all becoming very good at backing up our systems to create resiliency and recovery capabilities. So now they steal all your data *before* they lock up your systems. Then if you refuse to pay, they release all that data to the public—the embarrassment is a second way to extort the ransom.

"Ransomware continues to be the top threat," Coombes confirmed.

The barrier to entry has lowered, since you can buy malware on the dark web very easily. Attackers are more aggressive, more stealthy, and fully cloaked. We've done a lot of work around ransomware: new technologies, new processes, a lot of training. We do tabletop exercises at the Board level. The biggest concern is our supply chain. We've seen a number of companies hit with ransomware, and that could lead to a big operational impact on our company.

The second priority is increased geopolitical tensions leading to cyberwar. We are keeping a close eye, especially with Ukraine and Russia. [*Note: Russia invaded Ukraine 15 days after this roundtable.*] Russia is not only threatening the US if we interfere, but just a couple of years ago Petya/NotPetya hit governments and large companies around the world, and a repeat could bleed into supply chains.

Finally, zero-day vulnerabilities have doubled since 2020. Organizations struggle to keep up with patching, Log4J is still challenging to find, and all those instances can be exploited.

"We talk a lot about how to stop the bad guys from doing bad things, but the primary concern is on the risk side," Bill Clark, Manager Strategy and Planning for Chevron, reminded the group.

What are the risks for organizations, for people, for IT environments? We see advances and sophistication by threat actors, and a lot of focus by them on process control networks, on OT. So our top priority is to stay ahead of them and protect our process control networks, because there is a completely new risk in terms of business disruption.

In the Colonial Pipeline incident, the bad actors got ransomware onto the business network and shut it down. So it wasn't a technical issue, it was a business process issue: If you can't schedule a pipeline, you can't run it, even if you are fully technically capable of

doing so. This showed the integration between the OT network and the business network, and the reliance of OT on business systems.

"Do you see these OT threats as real?" asked Hans Brechbühl, Director of the Digital Strategies Roundtable. "For example, we all see business email compromise, but have you seen actual penetration into operational environments?"

"We've never had an internal OT incident," McIntyre answered, "But yes, we've had to help customers who've been compromised after they bought our equipment but not our services, and then didn't set things up properly."

"We see third-party equipment come in with malware already embedded," declared Ray Huber, Senior Vice President of Information Technology at Eaton Corporation. "They're trying to get into the lowest level of automation, and then work back into the rest of the infrastructure. OT threats are very real."

Damned If You Do…

"What principles do you have for handling a ransomware incident?" Brechbühl inquired. "For example, when Norsk Hydro was attacked, they established a set of principles immediately:

1. We're not paying.
2. We're going to run all our factories manually.
3. We're going to use text & social media internally to run the company.
4. We're going to do public updates every day.

"There are different variables," Huber suggested. "If it hits just one site, we can contain it. If it spreads to other sites, that's a factor. How big is the ransom demand? If it's a manageable number, it might be better to just pay it. No one wants to pay, but that may be cheaper than being down for two weeks."

"Colonial paid right away," pointed out Maria O'Neill, CIO of the American Bureau of Shipping.

> Colonial wanted the optionality, because they didn't know if they could recover. Our policy is to inform a board subcommittee immediately, because our CEO needs their guidance. Our starting point is to not pay, but we don't know what the circumstances are going to be.
>
> For instance, as is publicly known, we were victimized a few months ago. We kept getting emails saying, "We have your data and we're putting it out there." And really, they were asking for very little money, but we just ignored them, and then went away. It's important to assess each situation.

Diaz raised an objection to the pay-sometimes approach: "Sometimes you can't pay because law enforcement won't allow you to negotiate with blacklisted organizations, and if you do, you can face criminal charges. Paying is not always an alternative, whether we would want to or not."

“When do you involve government agencies?” asked Bill Braun, Chevron’s CIO. “You may get some benefit in terms of intelligence, or help recovering your ransom, but you lose control of the external information and communication.”

“The agencies say to call them immediately,” answered Ngozi Eze, CISO for Levi Strauss & Co. “On the one hand it’s very important not to run afoul of OFAC regulations. If you pay the ransom, then you’re effectively funding criminal enterprises. But on the other hand, as soon as you call them you lose operational control—it’s their case, and you’re along for the ride, when what you want is to maintain maximum flexibility for your decision makers in times of crisis.”

“I’ve heard that many companies are not buying cyber insurance because the cyber insurance companies require you to notify them immediately, and they take over the response. Is this a fact?” O’Neill asked.

“There’s a lot of gray area if a nation-state is involved, and the insurance companies will push back,” explained Adam Golodner, CEO of Vortex Strategic Consulting and Executive Fellow of SDA Bocconi’s Corporate Information Security Roundtable.

> Most policies have exclusions for acts of war or terrorism, although you can negotiate these out. The other complication arises from the OFAC sanctions, since the US government has prohibited doing business with anyone on the denied persons list. The question is, “How do you know if the person demanding the ransom is on the list?”
>
> The government says, “You should tell us before you decide to pay. But even if you tell us, then we won’t tell you, because we can’t predetermine if they’re on the list or not. But thank you for letting us know, because if you do pay them and it turns out that they were on the list, then you’re still in trouble, but maybe not as much trouble as if you didn’t tell us.” There’s a lot of gray area here, and the cyber insurance companies are subject to the same laws and ambiguity.

“It matters if you are buying insurance to pay the ransom, or to secure the response,” asserted Steve Zerby, CIO of Owens Corning.

> Many of these companies have negotiated agreements with forensics teams, negotiating teams, Bitcoin specialists, in terms of where they are in in the queue in case something happens. It’s like having a Navy SEAL team on retainer: Imagine something has infected a hundred companies, and you need a Bitcoin specialist from Crowdstrike *right now*. Are you Number 1 in line? Or Number 100?
>
> There are pros and cons to cyber insurance. Some people believe that if you don’t have insurance, you’re a bigger target, because your ability to respond is not as proven, not as seasoned, so you won’t be able to recover and you’re more likely to pay. The other point of view is that if you have insurance, then you have deeper pockets, and you’re more likely to pay.

Phishing Lessons

"How are organizations mobilizing to deal with this new threat landscape?" Brechbühl asked. "What are the details that make companies successful in their security efforts?"

"We started by taking a very draconian stance on business email compromise," began Mindy Simon, Chief Global Business Officer and Information Officer for Conagra Brands.

> When a third party gets compromised, we cut off email. Hard cut. Our business partners have to go to Teams with that party until we get confirmation that the incident has been contained and remediated. We also will not change any master data in AR/AP without doing a verbal confirmation back. And if no one answers the phone number that we have on record, we won't make the change.

"We also took a tough stance," concurred Twila Day, CIO of Huntsman. "We had a lot of repeat offenders in phishing campaigns, and some of them weren't even taking the training. There was a high-level conversation, and now if you don't do your training, you don't get your bonus. It's all or nothing. On the other hand, the training was dry and awful, so we gamified it."

"We had typical PowerPoint decks and email newsletters, and they just don't get a lot of engagement," continued Day's colleague Ginsburg.

> This year we made a virtual escape room, where you had to solve cyber puzzles to get out. We created a virtual scavenger hunt, and other little games. We focused awareness each week around a key change we wanted to enact in employees. Instead of focusing on teaching about ransomware, we focused on the behavior we want you to change. Re-booting machines was one of those; understanding that anything you put on the Internet is forever was another.
>
> What got the most engagement was the contests. People got points for completing the hunt, the escape, and depending how many points you captured, you got put into a raffle for gift cards. At the top tier, people who got perfect scores received cash prizes. The outcome was that more than 80 percent of our employees participated in at least one of our October cyber awareness activities, and well over 50 percent participated in at least half. Those are huge increases from prior years.

Braun described a different approach:

> We've switched most of our compliance training to be able to test-out at the start. The questions rotate, so everybody doesn't get the same set. It shows immediately how well people are retaining the information, and for people who do retain, they don't have to sit through the 30-minute video. You can imagine how seriously people focus on the questions!

"We require all 280,000 people to take the awareness training every two years," explained the Nestlé Group's CIO Chris Wright. "We also do a lot of global phishing campaigns, and we know that people who take the training are three times more likely to report phishing incidents. And the

awareness part really matters, since at last count 70 percent of our security incidents relate to forms of social engineering."

"Click rates in phishing simulation are important, but what's even more important are the reporting rates," added John Peterson, Nestle's Group CISO.

> When you delete something suspicious without reporting it, you might protect yourself, but you're not doing the company a favor. We'll never eliminate phishing—there will always be a part of the user population that will click—so we focus on reporting, and we try to get people to change their behavior by rewarding them, rather than by penalizing them.
>
> Users are often in doubt about whether the mail is legitimate or a phish. We don't want people to try to figure it out by themselves, but to report it. So we put a lot of effort into giving users a fast response. We have an ML engine in place, so even if a thousand people report the same email, it doesn't create more work for us.

"Has everyone embedded a phish button?" Simon asked.

"Yes, but let me build on that," Braun answered. "Our phishing rate has been going the wrong direction, and it's predominately people on their phones. We haven't solved the phish button on the phone. It's there, but it takes 4 or 5 clicks, and so no one does it. They either open or delete. Has anyone solved phishing on the phone? And do you see a higher phishing failure rate on phones?"

"We do, and a lower reporting rate," Ginsburg confirmed. "That's why just deleting is not good behavior: If you're the first person to get a phish that went to all executives and you delete it rather than report it, then the second person to get it will fall for it. If you report it, and we recognize it as a phish and take it out of the inbox, then no one falls for it."

Alice Crippa, Security Consulting Engineer at Cisco and recent Bocconi MSc graduate in Cyber Risk, summarized findings from her thesis on phishing awareness:

> Employees generally are over-confident that they are less likely to be involved in a negative event, whether that's a car crash, a physical virus, or an online scam. So in phishing awareness programs, it's vital to create a new culture that rewards the behavior that we want in the workplace, since more and more daily work is being accomplished digitally and online.
>
> Another finding is that unless phishing awareness programs are integrated with technology measures and appropriate security frameworks and policies, they become less and less effective. A click rate below 10 percent is very difficult to achieve with static awareness programs —employees get accustomed to the content. Two solutions that do help are threat intelligence and machine learning. Sharing threat intelligence among companies has been proven to be successful, but many companies, especially in Europe, still don't share, for fear of negative publicity and/or legal and privacy issues.

> Machine learning helps in detection, and also in the customization of awareness programs. For example, younger people may be more vulnerable to Netflix subscription emails, versus Amazon for older people.
>
> The final point is that smishing and vishing are becoming challenges. SMS and voice calls are the next threat vectors.

"We've had several reports of phishing through WhatsApp, or just straight texts," acknowledged Stephen Cicirelli, CISO for the American Bureau of Shipping (ABS). "When we get a notice from more than one person, or more than one region, we put out a company email: 'This is what's going on. We don't do business over WhatsApp; we don't do business over text. Use official communications channels only.'"

"What are you doing for OT teams in terms of education?" Brechbühl asked. "Are you doing any special education for that group, as it becomes more and more at risk?"

"We target by level," Diaz answered. "Executives and line managers get personal conversations. Then we do more technical training: What you have to do, what your assistants need to do. When we started in the plants we received a lot of questions, and it has really made a difference over the last two years."

"When we first started our OT security program, we sent a couple of engineers to class at Idaho National Labs, where they got to do hands-on attack and defend of OT systems," Townley added. "That experience got them to buy in, and understand the risk. More recently, as we've developed OT security centers, we made sure to target training at our people in our plants who buy and support OT equipment."

"What about carrots and sticks in phishing awareness programs?" Brechbühl followed up. "A carrot is kind of a free thing to do; what is the consensus on sticks, and the size of the sticks?"

Simon described one of Conagra's "carrots:"

> Our CEO had the idea of introducing "cyber champions" in every company Town Hall. People are nominated for doing something great in cyber. We choose one from a plant location and one from an office location each quarter, and what they did is presented in a 2-minute video by our cybersecurity manager during the 45-minute Town Hall, with the whole company watching. It's been a great success.

On the other hand, Chevron's Clark presented a stick:

> We had an "accountability model." We had one for regular users, one for privileged users, and one for contractors. The number of times someone clicked would cause a penalty, which was usually removing network access. We worried that the penalty was too strong and counterproductive, so we took it away—and phishing got worse. So we're now re-thinking how to implement accountability. The stick is coming back.

“Our board did ask us to put in penalties for repeat offenders,” O’Neill reported. “The problem is, that’s not our problem. We’re trying to solve for the high number of hits in any given test. We are going to roll out a program with penalties for repeat offenders, but we really don’t have very many. If someone fails once, they’re already getting really nervous—we don’t have anyone who’s failed three times in a year.”

“We can do training, we can prepare employees, but this is one of the biggest risk areas for employees,” Day demurred.

> If you have someone who is repeatedly failing, the penalties have to include everything up to and including firing, because it’s too big of a risk to keep somebody who doesn’t understand the importance of taking the necessary steps. When we started reporting back to management teams, “Here are your repeat offenders, the next steps are penalties on performance and money”—that’s when we got a direct correlation to improved performance on phishing campaigns.

“The penalties are what caused behavior to change,” Day concluded. “It can’t be just my responsibility, or the CISO’s, to counsel people—the leaders of the department have to hold their people accountable. When you enforce that, that’s when you see the change. Nobody wants to have to deal with it, but it has to be dealt with.”

Cloudy Forecast

The discussion shifted from employees inside the enterprise to partners outside the enterprise. “Let’s start with the cloud,” Brechbühl proposed. “What are the novel challenges that cloud services and operational integrity in cloud services pose for cybersecurity organizations?”

“Where is the company *really* located?” Cicirelli suggested. “It’s so easy for a vendor to look perfectly legitimate, but you’re turning over all your IP to them, and maybe they are in an embargoed country. You’ve got to dig into that.”

“In our early cloud days, we tried to replicate all our same on-premise controls in the cloud, and that was a bad idea,” Braun recalled.

> For example, we do a fail-over test every six months for Tier One systems. What does that mean in the cloud? If I’m paying for redundant Azure services between zones, do I need to test that? Does Microsoft test that? I’d rather Microsoft verify that they’ve done it rather than have all of us do it independently—that doesn’t make any sense in the cloud model.
>
> But it’s a change: what if our auditors say, “You didn’t do your hot standby test on this critical system.” “No, but I do have a certified statement that Azure did the test.” Is that going to work? It’s a whole different way of thinking, about expectations and audits, and it’s not all sorted out yet.

“Two things shift when we look at cloud services,” Ginsburg stated.

> On testing, I completely agree: We’re moving into a verification role. We verify that Microsoft has done the test; we don’t run the tests ourselves. The other is that too many people, especially at the executive levels, look at cloud as an off-loaded risk: the cloud vendors are expected to provide business continuity, disaster recovery, resiliency planning, data protection.
>
> But if we haven’t contractually obligated them to these responsibilities, with penalties for failure, with SLAs that have very strict requirements, then we haven’t offloaded anything. We still have all the dangers, but less control, so we’ve actually *increased* our risk. Many of these cloud services aren’t as well-documented or as contractually obligated as we would like them to be.

“Some of these cloud vendor contracts have been in place for a long time, and they need to be re-assessed,” Day added. “They don’t contain the same requirements that we need today, or what the penalties are. It’s hard to hold the providers accountable.”

“And as these contracts age, the vendors are starting to separate resiliency services to monetize them,” Simon pointed out. “So now the same service costs more, because they’ve separated the redundancy.”

“You can put in the right contract language with the bigger ones,” Cicirelli noted. “It’s the smaller companies, that people put on their P-cards or are free, that are tough to control. There are so many apps available where people can put information: brainstorming apps, mind maps, apps for a quick meeting, especially now that we’re remote and don’t have whiteboards to talk around. These are much more difficult to manage.”

“Extending security into the cloud is really a challenge,” Eze agreed. “People are just trying to work harder, better, faster, smarter, but they end up leaking confidential information to a vendor that you don’t have a contract with to even look at their security controls. These project management tools and presentation tools are the most significant challenge of data governance as it relates to security in the cloud.”

Wright supported Eze’s point:

> Moving to the cloud meant that we have had to completely re-think how we monitor and manage, from crisis management to end point monitoring and everything else. And for anything critical, we don’t migrate without SSO.
>
> We’ve done a bit of consolidation with cloud vendors over the last few years. Doing hundreds of partner certifications and chasing all the contractual information is really tough, but it’s easier with the big ones, since we work with them at scale across many applications and very globally. That doesn’t make them all perfect, but they do strong auditing, since any issue is reputationally very damaging to them.

“A lot of innovation comes from smaller companies though,” Brechbühl observed. “What are the trade-offs in heading towards the larger companies? Can you work with younger vendors to help them bolster their security and create a win/win, or is that a pipe dream?”

“That’s tough to figure out,” Braun admitted.

> How far do start-ups have to progress before they get to work with us? And then how much is left to scale up to the enterprise? We used to have a high bar, and vendors had to do all kinds of work to meet our standards just to run a pilot. Then two days into a test, it’s a disaster, and they’ve wasted three months of effort and hate us. The other approach is to let them play in the sandbox, but then even when it looks promising, they have six months of work to do to get a deal. They don’t like that much, either.

“We sign off at different levels of risk,” Wright explained. “If we’re doing a pilot with one brand or one market, and it doesn’t present a major consumer risk or could cause the broader business to fail, then we’ll accept a risk-based signoff from the product leads. At the point it becomes operationally critical to the broader business, then it has to go through the hoops. We find that’s a useful checkpoint, because sometimes you find it’s not worth it and you kill it without doing all the work.”

“We do business impact assessments and privacy impact assessments on all cloud solutions,” Petersen added. “The level of criticality determines the level of controls that are required.”

“Innovation is only interesting if everybody gets to use it and it actually produces something,” Zerby pointed out. “We’re not a big enough company that you can sustain yourself by having just us as a customer, so you might as well get through the risk hoop: it’s the only way you’re going to gain market share anyhow. If we can help you accelerate that by being a pain about security, we’re happy to do so. We don’t win many popularity contests with this point of view, but risk management has to come first in a large enterprise.”

Petersen followed up with a question: “When you first sign a contract with a cloud provider, you go through a rather thorough assessment. You then have a three-year contract, and things may change over those three years, in terms of architecture, the nature of the solution, or other things. Beyond SOC reports, how do you keep an eye on managing the re-certification of solutions in terms of how they may have scaled or things may have changed?”

“We keep an inventory of our cloud solutions, and if they’re rated as high risk, we go back annually to the business owner,” Townley answered. “Has the scope of how we’re using this system changed? For example, when we evaluated it, it didn’t allow file uploads; now they’re updating all kinds of files. We survey annually, just to see if we need to re-visit anything.”

“We also tier our providers in terms of risk,” Ginsburg assented.

> We have a two-year cycle to make sure they are still tiered correctly. Sometimes one business unit started using something, and it was a low-risk use case. Three years down the road, two other businesses are using it for higher-risk issues, but we still have it tiered

> as a low-risk entity. So we go back and re-certify: new questions, third-party audits, the whole process.
>
> We also use BitSight to monitor our high-risk vendors. They continuously monitor the external presences and look for vulnerabilities and issues. And we use OneTrust to do a lot of risk assessment and due diligence, since they've already looked at vendors a hundred times over for other clients—they don't have to re-do it just for us. They're able to do it more efficiently and at lower cost than we ever could.

In What Do We Trust?

"The concept of how one determines whether or not a product or a service or a company is trustworthy is at the heart of this conversation," Golodner observed.

> How do we as *users* of products determine that? How do we as *producers* of products represent that to our own users? They're two sides of the same coin: are there specific, intractable conditions of trustworthiness, across product development and supply chains and corporate governance, that cause someone to believe that a company is trustworthy?

"As a supplier, we receive humongous papers and requests from our customers to our cybersecurity folks," began Alejandro Lammertyn, Chief Digital and Strategy Officer for Tenaris, "They're all very generic. We dedicate a lot of time to answering these questions, but they're so generic, the companies are just protecting themselves against fault, not against actual hurt."

"We do have lots of smaller customers that just find a paper somewhere online and send it," agreed Mark Meyer, Tetra Pak's VP, Global IM and Process Office.

> But we also get intelligent questions from well-functioning customer organizations. With the big customers, we know what they're asking, and why, and we have a mutual interest to make it work. But how do you create a set of custom answers that work for everyone? And then the landscape changes…. We've wondered if we can write a statement that addresses at least some percentage, and say, take it or leave it. But we also know we have to be adaptable, because the bigger, more complex customers have good reasons to be asking the questions.

"The problem is, what are the real indicia of trust?" Golodner proposed. "In performing due diligence, I always end up doing something that completely doesn't scale—I get on the phone with the CISO, and I figure out whether the person is clueless or clueful:"

> What are your operations like? How many people on PSIRT, do you have a CSIRT? Does someone have a Stop button if software is going out with a security problem? What are your relationships like with governments? Where is your stuff coded, what government laws do you operate under? How involved is your board? Yes, you filed the GDPR, but where does my data actually *go*? Are you selling it? To whom?

"Things are inevitably going to go sideways," Golodner finished. "When things do go sideways, does this company actually know what to do?"

“I do the same thing, but I’m more simplistic,” Zerby laughed. “I just ask, ‘let’s walk through what happens at your company’:

> “Tell me about your email filter. Do you have an EDR on the PC that emails are opened on? Do you have Office configured not to open an automated script? When’s the last time you looked at hardening your AD? Do you have honeypots that tell you when someone’s looking for files?”
>
> I either get thoughtful answers, or dead silence, or objections. I go as far as I can, and then I ask myself, does it all hang together at the end? That’s the only way it really works. Each conversation takes an hour, two hours. To do our major vendors dedicates two days. That feels like about the right level of investment.

“So is this a behavior around CYA, or are we actually trying to figure out if we can have a trustworthy relationship with these people?” Brechbühl wondered.

“And what do you do with all the information?” Simon added. “Do you say no to suppliers? Do you ever turn down customers? Or do we log all of this because it makes us feel better to know?”

“We have kicked suppliers to the street,” Cicirelli affirmed. “But mostly what you want to do is create a better contract in order to mitigate potential points of failure. It’s harder when you’re the supplier, though.”

“Of all the security challenges, this is the most challenging,” Eze concurred. “There’s really no way to find a residual level of trust with our vendors that we feel confident in. It comes back to the ability to have the appropriate legal language in the contract for indemnification, and the ability to do follow-up audits, because outside of those, it’s very difficult to get to a comfortable place.”

“We all spend way too much time on this process that has almost no value,” Huber bemoaned.

> If the business really wants the technology, they’re going to find a way to acquire it. So how much time should we be spending? Should we evaluate all the questionnaires? Or evaluate some proxy, like ISO certification? Those can all be manipulated. They’re just a bunch of check-the-box questions, and what are you going to do if you get an answer you don’t like? It goes back to the trust relationship: I’m going to have a conversation with this person, and see if I feel that I can do business with them or not.

“We’re all asking the same questions of each other, multiple times, point to point. It must be 80 percent duplication, hundreds of times,” Wright offered. “So now some vendors are paying to get certified by us, and then they use that certification with other customers. It’s actually helping to avoid quite a bit of waste. The industry moves so fast that it’s very hard to create a certification standard that stays up to date. But I’d sure like to not have my team spending time asking questions and doing assessments.”

Clark added another level of complexity: “Assessment and certification is one side, and technology is another. Many of the products being provided to us are insecure. What can we do as a group—

because individually, it doesn't seem to work—to convince the vendors to provide us products that are secure by design, and then secure throughout the life cycle?"

"Those are two different questions," Golodner answered. "How do we ensure that what they're providing in the first place is secure?"

> Good news on that front: Some of the White House memoranda and the TSAs that have come out post-Colonial Pipeline have focused on that, and CSET has been charged with developing standard processes for software suppliers to get their products certified. On our end, we'll have to ensure that we're only using software carrying those certifications. We're six months to a year from having that standard worked out, but it's on the horizon.

"But for the ongoing piece…." Golodner shrugged. "I don't have a good answer."

The New Generation Gap

"We've talked about different threat environments, and the external landscape," Brechbühl recapped. "What capabilities are you adding internally? How are roles and processes changing?"

"We are moving cybersecurity into our agile development processes," Clark answered.

> Security used to be at the end of product development: We would get a new app and send it to the security team. They would say, 'Wow, this is very insecure," and send it back, which would create tension between teams and was very inefficient. So we moved security-by-design to the front of the process. Development now partners with security personnel, security architects, and engineers in vulnerability management. They work together to bake security in from the beginning.

"Physical security," Wright suggested. "Increasingly, our cybersecurity services are being asked to investigate things related to physical threats, and people who understand both worlds are key. Another gap is specialists who really deeply understand the China ecosystem, down to specifics on how privacy has to be handled there."

"We are trying to add people who are interested in policy standards and risk, and also have enough technical background to evaluate equipment," Cicirelli offered. "But we're having trouble finding them: most IT people are really into IT and aren't interested in policy. And most people who are really interested in policy and governance typically aren't that interested in the inner workings of IT."

"It's a challenge to find people in every area," Huber agreed. "Like everyone else, Eaton struggles to recruit. We have had some success working with universities that have cybersecurity as a discipline. We bring them in as interns, and if we like them, we don't even let them interview: we make offers right after their internship."

"We often hear questions like, 'How can I have a cybersecurity career in an oil and gas company?'" Clark said. "So we built out different career paths—senior pen tester, senior malware engineer, senior forensics—to help them see the answer. We haven't gotten anyone through the whole path

yet, but it shows them that there is a future for them at Chevron, they can stay here, in cybersecurity, for an entire career."

"Even when we do find the right people, it's very difficult to retain them," Diaz lamented. "We find that the new generation, the young people, don't care that much about career opportunities. They just want the money. They are such scarce resources—we lose someone every week. They get offers for more money at Amazon or Google, and they leave instantly."

"Over-specialization is a big problem for many of them," Licato observed. "They want a different experience that allows them to expand beyond a narrow focus, a rotation program or similar. So we give them ten different things that they have responsibility for, and that keeps them involved."

"Especially people early in their careers, they want to see their progression noted—position recognition for sure, but also monetary recognition," Meyer stated.

> In India, for example, we're considering moving away from an annual salary review to twice a year, just to keep up with the market. We're not waiting 12 months to tell them they did a good job, so they should stay. If we wait that long, they're probably gone. But if we keep affirming that they're changing, they're growing, they're moving forward, then maybe they don't have to go somewhere else, they can do it with us.

Simon underscored Meyer's point: "We've adjusted compensation three times in 12 months. Especially at the lower levels in cybersecurity, they're getting the certifications. We train and grow them, and that quickly leads to an imbalance of their skills and capabilities relative to market comp."

"Salary is on one factor," Day agreed.

> But we also hear a lot of work/life balance complaints from people who are leaving. This generation is just as concerned about balance as they are about money, and they do not care about staying at the same company. They don't even care if they hop every year or two. They don't see that as a negative.
>
> A lot of people reassessed what is important to them over these last two years of the pandemic, and they're no longer willing to make compromises. This is a tough, competitive hiring environment, and our talent pool is not other chemical companies, or even Houston. Businesses have to be more open to new and different styles of work, and connect with the talent where it sits.

"We found three key indicators in a project on talent retention in cybersecurity," reported Silvia Belloni, Master's candidate in Cyber Risk Strategy and Governance at Bocconi University. One is professional development: training, certifications, and the like. The second is exchange programs: the ability to move across organizations to work on a project for six months, or to go abroad. And the third is a shadowing program, especially for those who are interested in having more managerial roles, or even in becoming CISOs."

“When you hire people, you have to hire them with retention in mind,” Zerby declared.

> Is the brochure that you’re recruiting them with really what it’s like inside your company? Because if not, they’re going to realize the mismatch in about a week. So figure out your brand, and be courageous about talking about it everywhere. A lot of people will run away from it, but when they run towards it, they tend to stick.
>
> Secondly, you have to work as hard every day to keep your employees as you’re going to work to replace them when they leave. What interests them? Do they want to learn more, learn less, stay in their role, take on a new role? If you aren’t in that discussion with them every day, you’re just asking for someone else to fill the gap.

Never Waste a Good Crisis

“With everything we’ve talked about—digital transformation, evolving threats, and so on—how are we addressing this changing landscape organizationally?” Brechbühl asked. “11 out of 11 companies here have the CISO reporting to the CIO. What are the driving forces to have cybersecurity structured this way, rather than being moved out of IT and into its own organization?”

“Chevron radically transformed the way we do digital last year, in order to increase speed to value and scaling across the company,” Braun responded.

> Our cyber team had been high-functioning, so we had to figure out how to put them into the new model without degradation—how to have the right cyber people plugged into the right teams to have the right influence at the right time? Our board did ask us to consider separating the cyber organization out completely. The primary reason to separate cyber from IT would be to make sure there is enough autonomous assessment of risk to put pressure on the IT group, so that cyber isn’t subjected to the broader IT will of the organization.
>
> We looked and recommended not to, in part because we didn’t have a separate risk organization. With direct reporting by the CISO to the Board, combined with independent financial authority, is enough mitigation to that risk. We now handle the cyber budget completely separately, with a different approval process from the rest of IT spend, so that they don’t have to compete with each other.

“Historically, Eaton’s businesses would fund everything for security,” Huber described.

> Sometimes security can really bring the business down, and so we struggled, the business units always want to delay one more year, one more year. But security and IT are so intertwined with each other. We reached the point of thousands of obsolete devices, and finally our CEO said “Enough, we’re centralizing it all, and IT is going to drive it.”
>
> Now we work with the businesses to allocate costs back, but they don’t make the decisions anymore. There still has to be a balance between what security is trying to do and what IT needs to do for the business. The CIO needs to make sure that all the aspects are being

balanced: We need to patch, we need to keep things secure, and we need to run our business, we need to keep all the machinery going. We have to have that balance, and the CIO is the decision maker.

"Huntsman faced the device problem as well," Day acknowledged.

We didn't have much of an organization, we didn't have many tools, we weren't spending money. At that point our Board didn't have any security expertise. The executive team thought we were fine, and there was absolutely no view into OT, at all.

I came in and said, "We have a big problem." At first there was no appreciation for the risk: "We're not a bank; why would anyone want to attack us?" Now there's greater clarity, especially on the plant side, in regards to risk, and we're in the fourth year of our global security project. We started by getting the global IT house in order, and now we've shifted to OT. Ultimately, we will pull in responsibility for OT into global IT.

"It's less about whom the CISO reports to, and more about the support from above," Day suggested. "Our Board member with the most background in security talks with us regularly—I know that if anything is happening on security where I don't have support from the executive team, I can go to the Board. Except I *do* have support from the executive team, and that has made all the difference in the world."

"At Tetra Pak we decided the mission of the central security team was to control and govern the cybersecurity landscape across the enterprise through architecture, capabilities, standards, tools, policy and procedure," McIntyre offered. "We partner with IT and the business through architects and coaches working in their teams to be sure from the start that they have the support they need. We provide brakes and guardrails, if you will, so that they can drive around the track faster. We try to help them understand that the responsibility is still theirs, and that we are there to help. We don't take responsibility away from them."

"Chevron has similar issues," Clark assented. "Facilities engineering is very relationship-driven, so for all new products being developed, we're partnering an OT security engineer with the development team. That helps us to build guardrails, and establish rules and standards: 'If you build it this way, you can still build it on your own, but you can also build it securely.' It's putting our foot in the door."

"Tenaris made the same decision, that IT should govern cybersecurity for both IT and OT," Diaz nodded. "Security just isn't a focus for OT, they are not interested in stopping production. So for physical plants, we took all the servers close to the lines and moved them to data centers. We virtualized them and made them redundant so that we can move the load, patch, come back, all without disturbing production. It takes a lot of money and a lot of time, but it's better. And once the production teams understand this and see the value, they start backing you up."

"Like others here, Tenaris has also passed the time of awareness of the problem," Lammertyn added. "Now everybody is looking to IT for help. But once you decide that IT has responsibility, then the question becomes, where is the budget? There is no OT security budget. Some is in

maintenance, some is in automation, some in other places. Now we have the mandate, we're still working on the funding, but we have to run it."

Meyer applied an old political dictum to the current security environment:

> We should never let a good event go to waste. Tetra Pak's team has been trying to just help out, to work on stuff outside of the mandate sometimes, and to become known as helpers. And then when an event takes place, we jump in with everything: first to solve it, and then to help understand how it happened. Then we can apply those lessons to say, "Here are good practices, and we need to view these things in a different way."
>
> We've had a number of these events. One was in a factory, and our audit showed the problem was everywhere. Then the businesses made the investments that were needed, but under our guidance. We can't own everything everywhere, but we create processes, procedures, guidelines, architecture—so that the businesses believe in them, or we're not going to get where we need to go.

"More than ever there's tremendous value in the approachability of your security organization," Zerby agreed.

> All the boxes are moving—now is not the time to be very black and white about who gets involved in what. If you build an organization that's approachable, so people know who they are and find them helpful, then they'll actually get invited into a lot of discussions. If people are comfortable inviting them to spend time in areas that may not be clearly security—those will be rich discussions. This isn't the end to how to solve the challenge of staying connected while all these pieces are moving and transforming, but it's really essential as part of it. If the CISO is inside IT, they're always in the conversations going on at the leadership level. I can't imagine having that office somewhere else, and missing all the infrastructure discussion that goes on. It would terrify me.

"A great CIO is a risk manager first, a talent manager second, and a tech manager third," he concluded. "If you get those out of order, you get yourself in trouble."

"The objective is to provide an ecosystem that balances the imperative to protect the enterprise with the need to adopt innovative, risky new technology approaches to remain competitive."
— Tom Scholtz, Distinguished VP Analyst, Gartner

PARTICIPANT LIST

Tackling the Cyber Challenge

Nico Abbatemarco	Junior Lecturer *SDA Bocconi School of Management*
Bill Braun	CIO *Chevron Corporation*
Hans Brechbühl	Associate Professor of Practice Director, Digital Strategies Roundtable *SDA Bocconi School of Management*
Stephen Cicirelli	CISO *American Bureau of Shipping (ABS)*
William Clark	Manager, Strategy and Planning *Chevron Corporation*
Chris Clark	Senior Vice President and CIO *Levi Strauss & Co.*
Jonathan Coombes	Vice President and CISO *Conagra Brands*
Twila Day	Vice President and CIO *Huntsman*
Gustavo Diaz	Senior Director, Information Security *Tenaris*
Ngozi Eze	CISO *Levi Strauss & Co.*
Adriel Ginsburg	CISO *Huntsman*
Adam Golodner	Executive Fellow, Corporate Information Security Roundtable *SDA Bocconi School of Management* CEO *Vortex Strategic Consulting, LLC*
Ray Huber	Senior Vice President, Information Technology & Sector CIO *Eaton Corporation*

Alejandro Lammertyn	Chief Digital and Strategy Officer *Tenaris*
Richard Licato	CISO *Airlines Reporting Corporation (ARC)*
Robert McIntyre	Director of Information Security and Information Security Officer *Tetra Pak*
Mark Meyer	VP, Global IM and Process Office *Tetra Pak*
Maria O'Neill	SVP and CIO *American Bureau of Shipping (ABS)*
***John Petersen**	Group CISO *Nestlé*
Mindy Simon	Chief Global Business and Information Officer *Conagra Brands*
Paul Townley	Vice President, Global Information Security *Owens Corning*
***Chris Wright**	Head of Information Technology and CIO *Nestlé*
Steve Zerby	Senior Vice President and CIO *Owens Corning*

*on Teams

Silvia Belloni	Student of the MSc in Cyber Risk Strategy and Governance *Bocconi University & Politecnico di Milano* Security Advisor *NTT Data*
Alice Crippa	Security Consultant Engineer *Cisco*