Center for
Digital Strategies
Tuck at Dartmouth

Cyber/Information Security in the Digital Age

A Roundtable Overview
European Chapter Discussion

Roundtable on Digital Strategies

Cyber/Information Security 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

Threats to enterprise information security are escalating due to a number of factors: increased connectivity with outside vendors; the growing number of network-enabled devices; the increasing number of human/device connections; and the enhanced coordination, sophistication and professionalization of security attacks. Members of the European Chapter of the Roundtable on Digital Strategies convened at LafargeHolcim's facilities in Zurich for a discussion of the current and future of cyber/information security. Topics for the day included current and future changes to the infosec threat landscape, and how enterprises can respond and adapt with technology, processes, and training. Participants in the session included CIOs and leaders of information security from Clariant, Hilti, the International Committee of the Red Cross, LafargeHolcim, and Swarovski, along with members of the Center for Digital Strategies at the Tuck School of Business.

Key Insights Discussed in this Article:

- **Cybersecurity is a growth market.** Cyber attacks are increasing in frequency, sophistication, and impact, as information security perimeters expand with new devices and cloud applications. IT and Information Security need to anticipate and respond with at least equal energy and innovation. .... **Pages 2 - 4, 6-7**
- **Changes in business practices are opening up the threat landscape at least as much as changes in technology.** The opportunities presented by digital and digitally-enabled services create a host of new risks; a key question for enterprises is how to balance the two .... **Pages 4-6, 7, 10**
- **"Information Security" has become a requirement that goes far beyond IT's ability to secure using technology.** Traditional IT security prevention and remediation remain critical activities, but awareness and training among employee, executive, and partner communities are equally, if not more, important .... **Pages 2, 5, 8-10**
- **Enterprises need to develop and implement business-based management and governance strategies for information security.** From prevention through detection to crisis management and remediation, Information Security is an executive staff/Board level responsibility .... **Pages 3, 5, 7-8, 10**

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).

“We Will Be Hacked”

“The one thing that keeps me up at night is cybersecurity, because the threat landscape has shifted so much in recent years,” began Volker Laska, SVP and CIO at Clariant.

> There has been a massive proliferation of social engineering attacks, and they’re getting smarter and smarter. They are evidence that security is not just about technology, it's really about people and behavior and awareness, or lack thereof.
>
> There’s also a massive proliferation of mobile devices, that are being used more and more in a mix of private life and business life. We now outsource more than half our work in IT, and we can see that our suppliers are increasingly targets for attacks. There is an expanding number of Internet-of-Things devices, and an increasing convergence of IT and Operations Technology, with more and more production networks being connected to commercial networks.
>
> These all add up to a huge problem in IT security. Since it's nearly impossible to build everything you need internally, you need to begin to depend on cooperation across companies, and industries, and external providers.

“We *know* that if somebody puts in enough effort, we will be hacked,” Laska concluded. “What we need to have in place is a strategy for how to get up and running again.”

“With all this proliferation, it becomes harder to define what is critical infrastructure,” added Yvon Le Roux, Executive Fellow at the Center for Digital Strategies. “What do I *absolutely* need to protect in case I am massively attacked?”

Valentin Simic, Director of Information Security at Swarovski, illustrated just how easy “massive” cyberattacks are becoming:

> There were 13 times as many cyber bank robberies as physical last year in Austria. It’s easier today to hack a bank than to rob one. The burden for such activities is very low, and it's becoming lower. You can download all the tools, and you don't have to have any kind of extra knowledge. You don't have to take any risk. You’re sitting in a country with low legal certainty, and you’re well educated, but you have no money: You might not have any reluctance to conduct such activities.
>
> That all combines into a threat landscape that makes it more and more difficult to protect from. I don't think anyone is able to protect against all threats. We have to face that this is not possible anymore.

Khushnud Irani, SVP and CIO at LafargeHolcim, described yet another new threat vector:

> You get a WhatsApp message on your phone, and if you download it, it goes through your calendar to see when you have meetings, and then turns on your voice recorder and even your video camera. You don't realize it, but all the content goes to the hacker — and depending on whom you're meeting with, this could be a significant eavesdropping risk. And it's clearly something that people are not aware is happening.

"Blackmailing is another one," Simic added. "They put a Cryptolocker on an office computer. It could be a file encryption, or it could be encrypting the webserver for a shop, and then you're offline. Instead of doing a DDS that could take a lot of resources — the risk the blackmailers have to take is basically zero. If that happened in our retail shops, it would have a real impact on our business continuity. We have to ask ourselves, 'What would it be like for us to pay instead of resist?' There is even a market now developing in Cryptolocker, for this 'ransomware-as-service.' You can participate, and if you succeed, you get a percentage of the payment."

"That's essentially a reputational threat," observed Hans Brechbühl, Executive Director of the Center for Digital Strategies. "You can recover the customer data; you'll still have it. But if they go public with it, is anybody seeing that happening?"

"That's a public nightmare, and your share price can take a nosedive," Laska answered. "I certainly don't want to read in the press, 'Clariant data hacked, CIO fired!'"

"I'm not sure about the impact on reputation anymore," Simic countered. "Three years ago? A nightmare, I agree. Today, I'm not so sure. There have been a couple of incidents recently, and the reputational impact has been zero."

"It's about how you react to it, right?" Irani asked.

> How to respond *should* be really clear, but in fact it depends on the situation. If people are hacking you, and the hackers have the ability to say so on social media, what is the appropriate reaction? If you are aware of the hack, should you tell people up front, or should you wait for the hackers to do so? Should you respond in the same medium as the hackers, or in a different medium?
>
> How you respond affects your reputation. There is a technique to what words you use, and at what point you communicate. Do you say "Okay, we are hacked," or do you say, "We don't know what's happening?" The words you use in social media really play a role.
>
> For the hackers, within the dark web they have a community where they feel pride, and they get awards and medals if they are able to hack larger organizations. It's something we have to be prepared for as enterprises: It's not a question of whether we will be hacked. *All* of us will

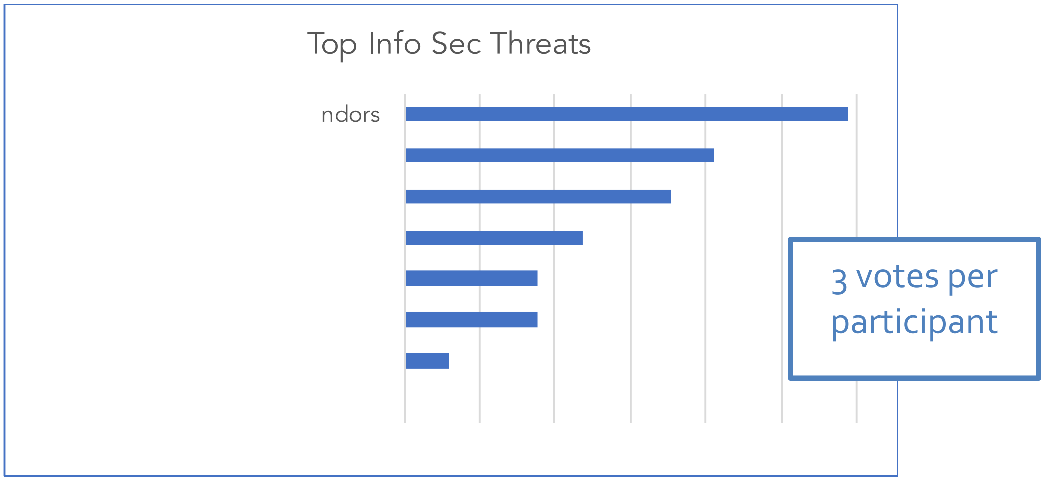
> be hacked, or we have already have been hacked and we are not aware of it. The question is, “How will we react? What is our crisis plan?”

“Cyberattacks are increasingly professional,” agreed Max Braun, CIO of Swarovski. “Attack-sharing in the social area is now often related more to awareness, and less to technical measures. Our consumers are very sensitive about personal data, and it’s not easy to find the right balance between privacy and enabling people to be mobile and having access to anything everywhere. So, we need to clarify what is our really sensitive data, and what we try to publish to the market.”

“There are a lot of complex items, linked across the entire organization,” agreed Martin Zehnder, Head of Enterprise Risk Management for Clariant. “The most challenging element is actually uncertainty. Things can happen, and we don't know yet what those things are. Our imagination may not be good enough for what we need to protect.”

Needed: Security by Design

Just as the evolution of hacking practices and technology is creating new risks outside the enterprise, changes in business practices related to digital technologies are creating cyber-risks inside the enterprise. Participants voted on the most important dangers.



3 votes per participant

Olivier Angyal, Head of IT Security Strategy for Hilti, listed four business trends that, combined with the evolution of the threat landscape, are changing their risk landscape:

- An increasing number of internal-facing applications;
- Our increasing use of cloud services;
- Active development of global operations and fostering of external collaboration;
- Empowering users to be more mobile.

“This is the picture that got our security investment plan approved,” Angyal explained. “We will

start with an IT security strategy, with a focus on global IT, and look at digital application software. But with so many topics, it's difficult to keep up with the pace."
"We are also doing more with digital solutions," Irani agreed.

> As we increasingly go direct, we expose ourselves via our banking systems to millions of retailers. So our surface attack area dramatically increases. We never had this situation with traditional business models. Our connections with suppliers are also increasing. As we connect to external firms, and globalize networks and infrastructure, our exposure to risks rises exponentially. What creates even greater concern is that investment in information security is not keeping pace with investment in digital business solutions generally.

Romain Bircher, Deputy Director, Communication and Information Management, International Committee of the Red Cross (ICRC) echoed several of Angyal's themes:

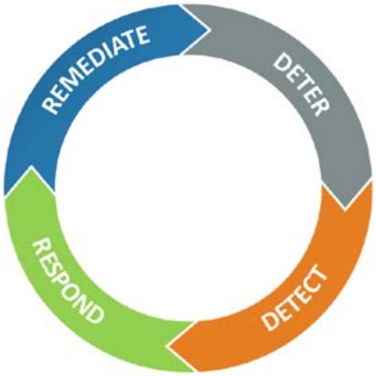
> Staff behavior is one of our major concerns. We have done phishing exercises, and the results were not good. We need to increase the staff awareness on social engineering and its risks related to cybersecurity. That requires the right methodology; it requires resources; it requires integration into training, and it requires practice at a wider level than has been done in the past.
>
> A second transformation at ICRC is the enlargement of our perimeter of information security, because we are enlarging the perimeter of our digital services. And a third issue is the tension between the traditional project model of development versus the digital innovations that we want to take advantage of. We need to get tools to people more rapidly, so they can test and innovate with a new technology, but we have a project process that takes time, in order to ensure the consistency of the data, data protection, and compliance. This creates tension. There is are opportunities for the organization, but also increased risk in terms of data security.

"We can forget about the old thinking of 'This is the boundary of my organization that I have to protect,'" Simic pointed out. "Security is now an issue at every point in the supply chain. We have more partners as more cloud solutions are being used, so now I need to care about partners: What *they* are doing with *our* data? Are *their* suppliers providing services in a safe datacenter? It's a whole new ecosystem, and there is much more to be concerned with than there used to be."

Laska pointed out the change in approach that the new threat landscape requires: "In the current world, you make people try things out, and security comes last. Then at the last minute, you struggle, and there's pressure to get things out quickly, and you start to make compromises. In the new world, you need to build in an *a priori* cybersecurity stream for your digital activities."

"We need security by design," concluded Amal Mezzour, Project Head of Group IT Security and Internal Control of LafargeHolcim. "You have to build security in from the beginning."

Re-Imagining Information Security



The group reviewed the cybersecurity model of Deter-Detect-Respond-Remediate that has emerged in recent years.

"We can no longer rely on preventative measures 100 percent," Angyal stated. "If somebody wants to breach into your network they can do it — It's just a question of how much effort. We need to re-balance our security priorities to have more of a focus on detection and response, compared to only prevention."

"One of the most important issues is the uncertainty," Georg Hünermann, Head of IT Governance/Group IT Security Officer at Clariant re-emphasized. "It's difficult to really know what's going on, and that problem is increasing with all the cloud services being brought into companies. We are implementing a Security Operations Center to increase visibility, because we get no good answers to questions we have."

"We also invested a lot in prevention and less in detection in past years," Mezzour agreed. "Now there's a shift to detection, because we need more capabilities to understand what's happening *now*."

> In one detection initiative, we search the Internet and the dark net for information that may have leaked from normal operators using private web applications. Their passwords and IDs get detected, and they are using the same passwords for personal applications as for our department. This gives us a lot of practical information to act proactively.
>
> We also monitor Google and the Apple Store for rogue applications that use our name but were not developed by us. We can take action on them, we can shut them down. And we keep an eye on third parties: Who are the key third parties that have access to our network? Have they been hacked? What vulnerabilities do they have?

"Detection can give us a lot of information that we can react to," Mezzour finished. "When there is a discussion on the dark web about your company, or you learn of another breach — you can take action, you can determine how to respond. The main objective is to reduce the damage."

"I like the idea of re-balancing," Laska admitted, "But prevention is still really, really important. One of the most important things is to have good and up-to-date virus protection, because that keeps out 90 or 95 percent of attacks. We should not let loose there."

"'Re-balance' does not mean we should move away from prevention," Angyal clarified. "It really is about finding a better balance: Bad stuff could be happening right now, and we wouldn't know. This is what happened with Target and other examples. When something is going on in your network for 12 months and you're not able to see it — we really can't afford that!"

"According to Gartner, the period of the average time of detection is around 300 days," Laska pointed out.

"That's because *we* are not getting more sophisticated," stated Irani, "But the attacks *are*."

> IT guys would normally be able to see that there's something crazy going on in their network, but the nature of the attacks has changed. IT can now go for 200 or 250 days without having a clue that someone is actually on the network. This is where you really need some other mechanism to be able to detect this activity.
>
> What is happening nowadays is not the "normal" type of attack in which someone just dumps everything and your IT systems can detect it. Instead, they break the attack into small chunks, somewhat similar to the Ukraine power grid attack, and that is much harder to detect and respond to. Detection and the like are things of the past: They are just basics we should abide by. The question now is, "How are we going to actually be able to handle these sophisticated attacks?"

"Maybe the focus is correction and remediation," suggested Tim McDowell, MBA Fellow at the Center for Digital Strategies. "It's more proactive than waiting for something to be detected."

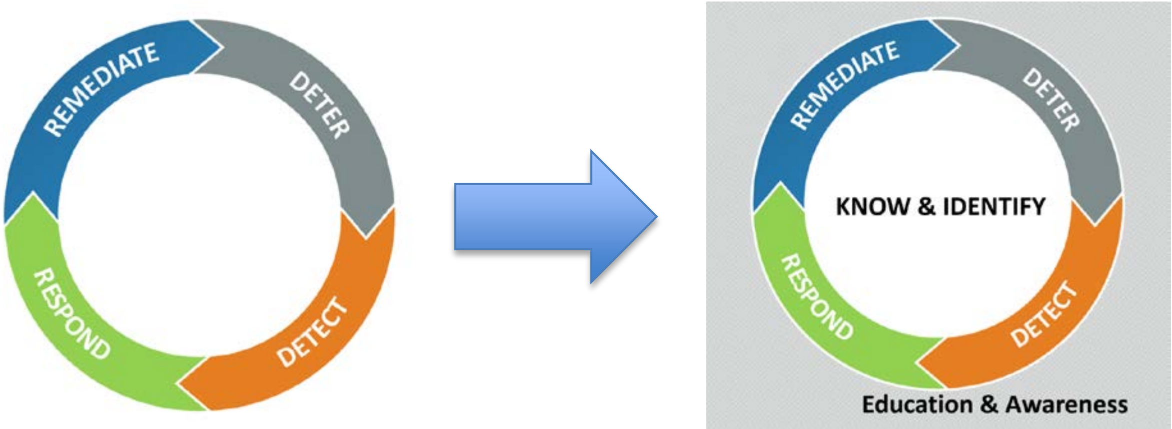
"'Respond and Remediate' should work for 98 percent, because the other 2 percent you honestly can't plan for," Simic rebutted.

> You can create as many plans as you want, but when something happens no one will pull out the paper to see, "Okay, what do I need to do now?" That's impractical and a bit unrealistic, and it can lead to focusing on the wrong risks. Recently I saw a funny risk management comic that made this point clear. Risk #1,422 was "alien innovation," and Risk #1,423 was "Building eaten up by giant pig." We need to be careful with what the actual risks are.

Brechbühl proposed an update to the DDRR model:

> There are two other big pieces we should add. The first is something like "know and identify." It has nothing to do with incidents, and everything to do with being aware of what you have: What is your critical infrastructure? What are the connected devices? Have you identified all your critical data, and where is it? It's a predecessor to the DDRR cycle: That's the right cycle, but if you have no idea what you have out there, it rapidly becomes an exercise in stupidity.
>
> The second piece, that needs to be pervasive throughout, is people education: Awareness.

> That's not just your internal people, it's also your partners. Traditionally we did well with building firewalls to keep people out. That piece is still essential, but it's shifted from 100 percent of the answer to something less than that.



"That's still the re-balancing idea," Hünermann affirmed, "But it also requires re-imagining information security within the company. The understanding has always been that prevention is something that IT does for us. IT will always tell us if there's something they're expecting, if there's something we need to do. If we shift the conversation to overall information security, that requires a set of actions and behaviors that cannot be done just by IT."

Who Owns Cyber?

"The key question is, 'Who is responsible for IT security?'" Irani asked. "We recently set up a war game internally, and I invited Legal, Compliance and Communications. The feedback was, 'If it's really an IT issue, do you think we should be attending?'"

> So we did the war game with all of them, and afterwards it was clear that cybersecurity is not just an IT issue; Communications has to be involved in cyber crisis management as well. We are used to crisis management in a specific country, or on a specific topic. But if it's cybersecurity, is Corporate fully prepared for how you actually deal with media? How we are going to react? It's a shared responsibility, and everyone needs to feel accountability. It's not just about protecting our systems technically.

"The chemical industry is quite risky, because of all the dangerous components, so Clariant already practices global emergency management," Laska explained.

> Crisis management doesn't change if is it a chemical accident or a fire. A cybersecurity attack would be an immediate global emergency, and all the people would be drawn in, with a special emphasis on Communications. There are logistical aspects, communications, legal, IT...

> And it's managed with military principles: There is nothing by consensus. There is one guy who calls the shots, and the others deliver.
>
> As part of these communications processes, people need media training. It doesn't matter if it's a chemical spill or a cybersecurity attack — they need to figure out how to communicate with the outside, and how to use social media, as the police have started to do quite effectively.

"*And* you still need to protect your systems," Bircher added. "You still need to remediate, you still need to manage communication, you still need to involve the business, because they are Operations, and business continuity may be affected, and they own the response. As you said, it's global crisis management, and not just on the level of IT."

"There was a time when IT security was 99% of 'information security. It's now probably less than half," Brechbühl observed.

"Organizationally, it's still 80 percent IT," stated Braun. 'Information Security' definitely goes beyond IT, but the majority of topics are still very IT-related, and the expectation from our Executive Board is that the focus is on cybersecurity. So the CISO reports to an Information Security Board, which consists of the CIO, the corporate counsel, and the corporate VPs for HR and F&A."

"What is the definition of 'cybersecurity?'" Simic asked. "Everyone uses the word, and everyone understands something different. Are we mixing 'IT,' 'information security,' and 'cybersecurity?' The old model was 'an information asset that I could protect,' and the criteria were the triangle of confidentiality, integrity, and availability. With the cloud, there may be no information asset per se, so the old triangle may not be sufficient any longer."

"'Cyber' would not cover a paper office," Laska observed, "It would not cover physical assets."

"The word 'cyber' is just not clear to me," Angyal agreed, "And it seems like it's only a buzzword. We separate information security, physical security, and IT security, which is part of information security. That structure seems much clearer to me."

Governance in the New World

Bircher described the ICRC's organizational approach to information security:

> We need to protect information in the system, promote education and awareness, and prevention intrusions and leaks. So we created a cross-functional board for Information Security, to which the CISO reports. But not only the CISO: We have data protection officers, so we can be sure there is alignment between information security and data protection

> compliance. We have the head of Information Management in the Archive Division, who is working on the typology and classification of information. A classification system is essential to giving people guidance on how they should manage information, and which kind of information they can share, according to which criteria.
>
> We also have a legal advisor for Info Sec reporting directly to the Director General. HR is involved for staff behavior compliance, and Operations is in charge of staff security in the field. We included all these key competencies to enlarge the scope of "information security" beyond the role of the IT.

"Our start with war games has been quite effective in raising awareness," Irani said. "We are also doing interviews with Executive Committee members, CEOs, and area managers, to give them more knowledge about cyber and what impact it could have. The conversations start them thinking a little bit differently. And we are making training certification mandatory for everyone."

"And when education does not solve the problem," Mezzour added, "There are other options. We are thinking of integrating the phishing alarm with the service desk. Mr. User no longer has to call the service desk to say 'I have a problem.' We are integrating the alarm with the e-mail system, so the user just pushes a button, and everything goes to the service desk, they handle the issue from there. Speed, ease of use — this can help users to contribute to security."

Hünermann gave another example of enrolling user support in familiar and easy ways: "We are publishing short stories on the intranet, based on cases we've seen. We tell the story in such a way that the reader asks, 'How could this have happened?' And we appeal to them by using the starting point of private PCs at home."

"It's all about lateral leadership and the ability to influence people and change their behavior so that they follow security policies," Simic concluded.

> How to do it depends on the culture, there is no one "right" recipe. In our company, the best way is to have people sitting in the same organization. We are physically close to each other, and so I can build up a trust relationship with our security managers sitting in the various IT departments. It's this trust that makes it possible to *not* have to enforce things with people, because they have created an inner understanding. But you cannot convince them without trust. If I had to design the security organization, the first question I would ask is, "How can I establish the trust chain?"

"It's difficult," answered Le Roux. "Security industry people are very guarded. They hardly talk, they hardly exchange thoughts, so it's really a challenge to build that trust."

"I fully support the trust mission," Mezzour agreed. "We need more people to bridge to the business. It's about risk acceptance, it's about understanding the business more so they can make decisions, because IT can't secure everything. We need more direction."

"There are different sets of risks and vulnerabilities, right?" Brechbühl asked. "We could shut down all digital, and we wouldn't have nearly the same degree of information risk. On the other hand, then we wouldn't be able to conduct business. These are the general business decisions that have to be made."

"Enterprise risk management is fussy," Zehnder answered, reflecting on the day's discussion.

> We need to be cautious about tightening security: If we eliminate all threats, then none of us will have jobs anymore. Risk is opportunity, and so all our business units have to take risks.
>
> What we need to look at is impact. Take the example of fake payment instructions: They're a hassle, but no one is going to transfer $500 million. If someone is stealing small sums, it won't kill our company. What is of enormous concern is if we can't serve our customers for a long period of time: That's very serious, and if there's also reputational damage, the impact could be enormous. The question is, "What risks are acceptable?" Then we do have to mitigate those risks, and that's why we can't sleep. So what most companies struggle with is how to define their risk appetites, and this is where the Executive Board, and even the Board of Directors, can contribute the most.

"We have a room full of stories here," he finished. "All of the benefits and all of the failures of our previous activities remain with us, whether we define ourselves as IT or as business."

Participant List

Cyber/Information Security in the Digital Age
6 April 2017

Olivier Angyal	Head of IT Security Strategy Hilti
Romain Bircher	Deputy Director, Communication and Information Management ICRC
Max Braun	CIO Swarovski
Hans Brechbühl	Executive Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
Georg Hünermann	Head of IT Governance, Group IT Security Officer Clariant
Khushnud Irani	SVP, CIO LafargeHolcim
Volker Laska	SVP, CIO Clariant
Yvon Le Roux	Executive Fellow, Center for Digital Strategies Independent Management Consultant/Advisor
Amal Mezzour	Project Head of Group IT Security and Internal Control LafargeHolcim
Valentin Simic	Director, Information Security Swarovski
Martin Zehnder	Head of Enterprise Risk Management Clariant
Tim McDowell T'17 *(observer)*	MBA Fellow, Center for Digital Strategies Tuck School of Business, Dartmouth College