CISO | information security workshop

The Intersection of Business & Security

Cybersecurity: Risks, Mitigation and Collaboration

A Workshop Overview

Center for Digital Strategies
Tuck at Dartmouth

Institute of Information Management
University of St.Gallen

Cybersecurity: Risks, Mitigation and Collaboration

An Executive Workshop by the
Center for Digital Strategies at the Tuck School of Business
and the Institute of Information Management at the University of St. Gallen

We convened a day-long workshop for Chief Information Security Officers (CISOs) at Kartause Ittingen in Warth, Switzerland. The topic of the day was cybersecurity. CISOs from industry and government joined with academics from the US and Europe to discuss the threats arising from the external electronic connectivity of the enterprise: What is their nature? What can be done to prevent them? If not prevented, what are best practices in remediation? And long-term, how can companies, governments, law enforcement agencies, and other participants work across company boundaries and across country borders to provide the best security possible for critical data? Participants in the session included private-sector CISOs from ABB, Adidas, Cisco, Daimler, Goldman Sachs, Hilti, Holcim, ING, Nestlé, Nokia, Novartis, Schindler, Swarovski, Swiss Reinsurance Company, and Thomson Reuters. They were joined from the public sector by representatives of the European Commission and the Swiss Confederation. The workshop was hosted by the Center for Digital Strategies at the Tuck School of Business at Dartmouth College and the Institute of Information Management at the University of St. Gallen.

Key Insights Discussed in this Overview:

This CISO Workshop publication is edited by Hans Brechbühl, Executive Director of the Center for Digital Strategies.

Introduction

The cybersecurity landscape has changed enormously in the nearly 15 years since the internet emerged from DARPA and started the world's second Industrial Revolution. With nearly 2 billion PCs in the world, more than 6 billion mobile devices, and billions more IP-connected devices, almost every piece of information worth knowing is somehow connected to the internet — and therefore accessible, if you know where to find it and how to get access to it. Alongside legitimate industries that have boomed in the internet age, cybercrime is thriving too: According to the 2011 Internet Security Threat Report[1] published in April 2012 by Symantec, one of the world's leading vendors of IT security technology:

- There are more than 403 *million* unique known malware variants, and more than 55,000 known malicious web domains
- Symantec software alone blocked 5.5 *billion* malicious web-based attacks last year
- 315 mobile device vulnerabilities were discovered in 2011
- At least 232 million identities were maliciously exposed in 2011
- The major US government defense agencies report an average of 10 million cyber-attacks per day, per agency (Source: DefenseNews)

In the face of this expansion in cybercrime risk and activity, CISOs of enterprises in every sector are scrambling to keep up with the criminals and protect their data. The challenge is enormous: sovereign states are moving into the cyber-espionage game as sponsors of Advanced Persistent Threats ("APTs"); organized crime around the globe is changing its business model to exploit cyber-vulnerabilities; terrorist organizations are looking at new cyber-based ways to wreak havoc. These entities appear to be quite willing to share new technology and "best" practices with each other. Meanwhile, their targets are justifiably cautious about sharing the same kind of information — and all too frequently remain stove-piped, independently fighting against a collaborating set of enemies. The criminals operate across borders with ease, while legal entities have to work within the regulatory, political, and legal frameworks of each nation in which they operate — which limits how enterprises and law enforcement agencies can enforce security and respond to attacks.

Eric Johnson, Director of the Center for Digital Studies, began the discussion by asking the assembled CISOs to describe the "one or two kinds of threats that you really worry about, the couple of things that keep you up at night."

Mission: Impossible

One participant stated the new reality of cyber-security as he sees it:

> The old doctrine was to have high walls and make sure people are kept out. In that model, you've got to address a complete range of threats, whereas the attacker can focus on one threat, and improve that threat to defeat any defense. We have to accept that our defenses have been and will be breached.

[1] http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf

John Petersen, IS/IT Security Manager at Nestlé, agreed emphatically: "Top management has unrealistic expectations. You *can't* have 100 percent security. It just doesn't exist, and they need to understand that. You can't mitigate all the risks. You *have* to expect that you will get breached. It's a matter of closing the gap from when you get breached until you detect them, in order to reduce the exposure you have as an organization."

ING's CISO, Ton Diemont, turned to more specific threats. "In the financial industry we see a tremendous increase in trojans and malware, hijacking the credentials of customers and really stealing money, so direct financial loss." Despite the fact that banks are 'used to' dealing with financial losses through bad loans, etc., the bigger issue for banks is retaining the customer trust and reputational risk of the banks in general.

Hans Brechbühl, Executive Director of the Center for Digital Strategies, raised the issue of advanced persistent threats (APTs), quoting a CIO friend: "'APT is a club that you don't want to be initiated into, and you don't really know much about it until you are initiated, and then it's too late.' Is that the general view of the room?" he asked.

"APTs are a fact of life," responded Steve Martino, VP of Information Security at Cisco. "We're all in the club, whether we wanted to be or not. And if some of you think you're *not* in the club, it's either because nobody's figured out yet that you have something they want, or you're wrong, because those are the only two reasons you're not in the club."

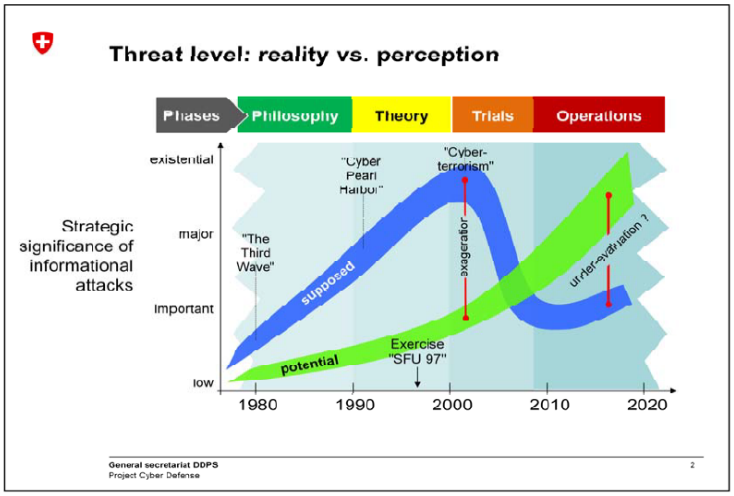
Scott Bancroft, Group CISO at Novartis, expressed the frustration of trying to provide enterprise security: "We try to find a way to make security a business enabler, rather than a hurdle. But in today's networked world, with the cloud, with consumerization, with nation-state attacks and hacktivism, all across a large and complex network…it goes on forever. Meanwhile the business demands that we must provide connections, at almost any risk, without understanding the risk that comes from the outside world. It can turn into the ostrich club: Stick your head in the sand and pretend it does not exist."

Jeff Moore, Senior Enterprise Security Manager at Adidas, agreed: "When senior execs hear 'APT,' they have just one concept of what an APT is. They don't have the concept as a complete end-to-end process: Plan-Research-Operations-Close Down. They have vendors saying 'We've got this product that will detect APTs on your network.' But how's it going to detect the guy who already works for the company, and *he* is the APT?"

Amal Mezzour, Global Information Security Officer for Holcim, sounded a note of caution about becoming too focused on APTs:

> Cyber-attacks are here to stay and will be increasing in the future, but we also need to have the basic controls that prevent against the most common threats. APTs are five percent or less of the overall threats, but we need detection control to be able to react fast. So there is a balance needed between preventive and detective actions.

Who's Afraid of the Big Bad APT?



Gérald Vernez is Deputy Director of the Cyber Defense Project in the Federal Department of Defense of the Swiss Confederation. In a presentation to the other participants at the CISO Workshop, Vernez suggested that perhaps for the first time, the threat of cyber-attack may actually be *under*-estimated. Vernez gave examples of new kinds of cyber-risks:

- A faulty software update led to the uncontrolled release of a large quantity of water at a dam on the Rhine River.
- Another faulty update due to the infected laptop of a technician took down the ticketing system of a major railroad, and another one brought down a major mobile network.
- After the crash of a plane in Madrid, malware was found in an important maintenance computer. It could have played a major role in this accident.
- Insulin pumps and pacemakers, as well as high-end automotive braking systems, are now easily reachable at distance or even connected wirelessly to the internet — the possibility now exists of assassinating someone remotely via software.
- The French naval airforce was forced to temporarily ground its carrier-based Rafale fighter jets due to malware introduced through an USB-key in their command and control systems. The same malware also hit the British navy and the German armed forces.

A key problem, Vernez suggested, is that "When it happens, you don't know what happened. You don't know if there was intent. Was the malware on the laptop of the guy who did a bad job there intentionally, or just by accident?"

Another participant explained one factor underlying the increasing risk level: "The attackers have become much more professionalized, whether they're criminals or governments or whatever."

Martin Sibler, VP of Information Security at Swiss Reinsurance Company, provided some detail:

> Virus scanners do not work anymore, because malware is getting too sophisticated. Even if you have several levels of virus protection in place, but some malware still ends up on the workstations. The bad guys are now using encryption techniques, as we do, to protect their payload from scanning when they download the stuff to the machine. What we've also seen recently is that they write their code into the memory — not to the hard disk anymore — so it's pretty difficult to detect it. If the users don't boot regularly, it just stays there. The latest virus attack we saw is really clever malware that detects whether a user is sitting in front of the computer. If you only scan the website with a virus scanner, no payload will be downloaded to the machine. As soon as mouse movement is detected

> — so that means the user is sitting in front of the machine —the payload is downloaded to your machine by encrypted channels, so it's pretty difficult to detect.

Valentin Simic, Corporate Information Security Manager at Swarovski, described how social attacks can combine with technology to make preventive security extremely problematic:

> Someone had a rental server in the cloud, and step by step they built up trust, saying, 'We are a design firm, and we want to work with you.' Emails went back and forth without any attachment, and then they started addressing several more employees, and started sending attachments. They got through one specific vulnerability in the first tier of anti-virus, but this was blocked by the second anti-virus. But they continued with this procedure until they found a vulnerability. They even prepared some websites that looked like normal sites, and were classified by the Bluecoat robot as safe. They really did a lot of things to try to make this attack a success.

Olivier Gourinchas, Head of Market Reach, Service Management and IT Security at Hilti, gave another example of a combined social/technical attack:

> We had users that were surfing on a website, and got a nice pop-up — "Your antivirus is not up-to-date and you may be infected." They thought that this information was important and forwarded it to their colleagues. So more people go on the website and click to get the update. For them, all looked fine. ... So now we are fighting against people who think they are sharing the right information with others, but they create security incidents because they have been misinformed or trapped.

Jeff Moore, Adidas's head of information security, described a similar infiltration:

> We found we were breached in a foreign country, though they hadn't gone far into the network. The way we found them was, when we scanned the network shortly after Microsoft had released the patch, these guys had already patched everything. They were the most up-to-date patch system in the network. So that made us look at a few other scenarios…

Eric Johnson, Director of the Center for Digital Strategies, observed a key change in the threat landscape, in the pervasiveness of APTs. "Five years ago, we were defending against scatter bombing techniques, but these examples of APTs seem very different. What is your thinking around defending against these very, very targeted kinds of attacks?"

Adidas' Moore described the difference: "Everybody thinks that APT is a zero-day attack, but it's not. An APT is a complete process, it's not a piece of software. People say, 'Oh, there's an APT on your network.' No, that was a SQL injection they've been working a long time to figure out to use it on the right system at the right place to get to everything else." He described a surprising discovery on the Web:

> We found a business case in PowerPoint in Russian. It was a walkthrough of what they were going to do to get at certain retail companies in the United States. 'This is what

> we're going to do; This is how we're going to target; These are the websites we're setting up.' They were going to set up websites in Asia, because the companies do a lot of business and a lot of manufacturing there. The *last* thing in their eyes was to attack with a zero-day. The plan even says, 'We'll buy the zero-day when the time gets close.' This was almost two months of prep work. They had names in the plan of *specific people*.

Mark Connelly, the CISO of Thomson Reuters, continued the theme: "The bad guys are very programmatic; they take a very long-term view on what they want and they know what they need to do. If they need to use some very sophisticated piece of software or technique — they use it only when they have to, because once it's out there, it could be discovered by others, and then it would lose its value."

The Case Against Mobile Devices

The proliferation of mobile devices — particularly in the Bring-Your-Own-Device ("BYOD") scenario — is one of the major drivers of change in the threat landscape, especially given the global and inherently mobile nature of it. CDS' Johnson asked the group, "What particular risks come straight out of mobile connectivity?"

Connelly from Thomson Reuters identified one key issue:

> The maturity around controls and technology that's available on systems is not there with mobile devices. It's a much more immature environment. Yet, there are more of them, and when they're connected to the network, they create a larger target surface. And a lot of times for some of the platforms you don't know where that code came from, and you don't know what's in it.

Scott Bancroft, Group CISO for Novartis, described some of the "small" gaps in technology that accumulate to create a large security exposure: "That space is a significant risk:

- Who built that code?
- What building blocks did they put in?
- What does it take to send it to a website in Russia, China, Nigeria — all of the usual suspects?
- Does the end user know about it?
- Are they deliberately sending your stuff about?
- Do you give them the option of a no-character password or a 12-character password?

"We all know which option the end user's going to take. Then it gets stolen, and now the question is, how much data was on there that matters, not the cost of the device."

"People don't know how to use mobile devices," Bancroft continued.

> We asked ten execs, and they said, 'Oh, I don't keep data on here.' 'So how would you open the attachments?' we asked. 'Well, I do it with Quickoffice.' So now they've got two copies of the file in there — a zipped and an unzipped — and it didn't look right on the display. So they open it in something else. Now they've got *another* two copies in

> *another* app. And now all of a sudden, you end up with a data spread that you've no idea of. It has never been easier to take information out," he concluded. "They're easier to carry. They're easier to lose. They're more attractive to a thief, and there are so many of them. So it's just more doors.

Nokia's Boije summarized the struggle to provide security while providing mobile-device users with the experience that they've come to expect:

> MDM (mobile device management) is in itself a good practice, as is application white-listing. Compartmentalizing personal data and corporate data allows you to do different things. But there are few good 3rd party commercial software security tools for the mobile device, and those that do exist, in my experience, kill the performance of the device.

Johnson asked how different organizations were dealing with the problem. One participant described the hard line that his company has to take: "Your employee device cannot be brought into R&D. When you go into R&D and you have a camera in there, you can elect to have the camera demolished or leave the phone at reception. In fact, if you ever want to use the camera again, you leave your personal phone at reception and don't use it during the day."

Petersen from Nestlé presented some other issues in mobile security, as developed by the group during a breakout session on mobile device & data security:

> Some organizations have an internal app store. Obviously, internally-developed applications are allowed on devices. Generally, everybody is allowing access to the Apple store. And *that* is causing a number of challenges for us, in terms of how secure these applications are. We need to push the app stores to make sure that they scan the applications, that they do *something* in order to give more assurance that the applications are actually secure and safe to use. There are new apps coming at such a speed that this is really necessary. In terms of the volume of applications, how do you deal with that? Do you black list? Do you white list? Another challenge with applications is licenses. When it's "Bring Your Own Device," and you download an application — if you use it professionally, are you violating the terms and conditions of the license agreement? But there's huge demand from the end-user community, and you just have to catch up. If you say 'No,' they'll do it anyway. We are just running behind and trying to catch up and find the best and most secure way to live with these things, but it's an impossible game. We can't really win this.

Enrico Senger, Head of IT Strategy & Transformation for Schindler, added to the complexities of setting mobile policy for global companies: "What data are you allowed to collect if you use mobile? Our subsidiaries are very interested in GPS tracking of the mobile workforce, but it's not allowed in Germany. It's allowed in Spain. You need a global solution, but you have to make sure that you are using the data in Germany the way that it is allowed in Germany, and to have a different subset of data that you can store and use in Spain."

"The bottom line," Mezzour from Holcim pointed out, "Is that there are different maturity levels. Some companies are just looking for a strategy; others have some solutions for some devices, but no one has a generic solution for *all* the devices."

Solutions?

Having discussed — though hardly exhausted — the topic of threats and attacks, the group turned to protection and remediation. One participant suggested a starting point: "There's a big issue of, 'What data are really worth protecting?'"

> We have a treasury department, and they have an availability issue, probably not so much a confidentiality issue. We have the annual report, which is an interesting example of how classifications with change: *Individual* sales figures are confidential. *Aggregated* sales figures are confidential up until the day of publication, and then they're nothing anymore. If we look at new products as an example, a drawing of a new design — at the right point in time — can be worth a lot. Experienced designers can deduce what the whole product will look like based on a little bit of information, so that's worth protecting, at least until the product becomes public.

Sibler from Swiss Re brought out the importance of understanding one's own data: "The businesses do not normally know what their golden nuggets are, so they do not classify the information, and they might not have monitors around them, as you would put around golden nuggets. If you don't know what the critical information is, it's difficult to find it, and to identify whether or not there has been a breach."

Swarovski's Simic emphasized the point: "In the past, things in IT were much more predictable. If an application was going to communicate, you knew what it was going to do in the network. You could say, 'OK, this is a good duplication, and everything else is bad.' Today you have to say that everything is probably good, and you have to identify the bad things. It is a dramatic change in the concept. Now we are trying to come up with detective measures instead of preventative."

Johan Boije, Director of Security & Continuity at Nokia, summarized the switch in approach that's needed to find a successful infiltration when everything on network appears to be legitimate:

> Most defenses are still built on the perimeter assumption, and in most of our cases, we should assume that we have been breached — that somebody is holding onto a little piece of our infrastructure or our applications. They maybe haven't come out of the closet, they maybe haven't done anything yet. What should you look for, in the event that somebody is going silently around our network? Because the traditional systems won't help us, since they will emulate the behavior of normal users. How do we look for those little signs of something odd?

Connelly from Thomson Reuters described one approach to supplement the perimeter problem:

> You can have a lot of perimeter fences, but the really good actors will find a way to get in without fighting those firewalls. They're going to have some social exercise, they have somebody click a link, and all those other defenses are moot. They're after access control and ever-increasing elevated rights. They understand your network better than

> maybe your own guys, and they find all your egress points. Then they can find the information they want, package it up, encrypt it, and ship it out. You don't know what they're looking for, but they do. Better control of your elevated rights is a nexus for solving one of the key problems. This is a very big concern with supply chain integrity. Find the weak point in the chain, and you're in. Control access and reduce elevated rights as much as possible.

To Catch a Thief

The group agreed that the current state of technology is insufficient to catch anomalous APTs. "Basic infrastructure can protect you from 95 percent of the malware," said Martino from Cisco. "It is the five percent of the attacks that are very sophisticated, where they spent months building on a reputation of a trust. … Do we have the right investigative knowledge to understand what's going on in the network? Because the way they attack, what they're doing, is about seizing control over a long period of time, probably years." Nokia's Boije concurred: "There is a lot of manual work to be done."

Markus Hänsli, Vice Director of the Federal Office of Information Technology of the Swiss Confederation, described the cyber-security team assembled to perform that manual work, and how they approach an intrusion:

> We have a small central search team — some 5 to 6 people — and a 12 or 15 person security team which we can assemble very quickly. There are specialists who analyze malware. There are specialists who analyze log files. We usually take guys from the customer whose data is affected — if it is — from system engineers, from operations — each guy that we need. We say, "Come on. We have a problem. You help us," and it runs perfectly. They come because it's kind of fun as well — it makes very good teams.
>
> When someone infiltrates you, it's like a chess game. You need to find the input vector — how he came in — and then start to look at what he does and to learn what he wants to get, what information he searches. Build up temporary measures to stop him part by part, and look at what his reaction is, learn what his motivation is, and estimate what his next step will be.
>
> The most important point is to control information, and you need to hold it very, very close. Every step your attacker is going to make and every step you are going to take to protect your information is part of learning the rules in this game — and it's a new game every time. It's a technical measure he takes, but it's some kind of an information grabbing movement — why does he do it this time? What does he want to learn? What else is he in already? You may see only five percent because you can't recognize him. You don't know what to look for, and so to learn from what he does is most important.

Vernez from the Swiss Department of Defense agreed with the objective proposed by Hänsli: "The technology is evolving and you use the techniques and the tools, as they are, but the most important thing is indeed the intent: 'What must the attacker breach to fulfill his own interests?'"

Cisco's Martino picked up on Hänsli's last point: "People tend to find an infected host, clean it, and say, 'Okay, that was the incident,' when it really *wasn't* the incident. You just found the one, so you think you fixed it. There are a *hundred* hosts that got infected, and you're not looking for those hundred. So we collect and maintain log data anywhere from 30 days past to a year past, to be able to go back and say, 'Okay, that's the signature. That's what I want to go look for. Let me go scan my logs and look for that happening anywhere else in the network, and then I can build a map that says it came in here.'"

Nick Godfrey, Head of EMEA Technology Risk for Goldman Sachs, picked up on the importance of pre-defined remediation processes:

> I don't know if you can prevent, but you can detect and quickly respond. If there's an attacker who is on the inside of your network and doesn't understand your environment, he'll be making noise that you can detect. If you can detect, you can respond, which is best done using pre-defined processes: If you have processes predefined, you can pull the trigger without having a conversation about it.
>
> If you have a fast response path that is relatively low-cost in the environment, then you can tolerate a certain number of false positives. Say, something bad happened on five workstations. You don't know what it is, but you don't like it, and you don't want it anymore. If you've pre-negotiated this, those workstations will just be blown away and the people will be given new images to work on.

Martino imparted lessons learned from building Cisco's version of a security team:

> A global single team manages all incident response. They are in two locations in the U.S., as well as in Asia, so we get around-the-clock coverage. We structured the team into analysts, investigators, and a small APT team. The APT team rarely works on incidents. They work on understanding what happened, how do I deal with it, what do I think might happen next — those kinds of things. The analysts take the many, many cases — the anomalies — and they decide whether or not an incident deserves an investigation. At a certain level they'll just handle the case, because that's the extent of it. Others they hand off to the investigative team, and there's a playbook of how it goes from analyst to investigator.
>
> The analysts primarily come out of IT or have technical backgrounds, and we teach them how to be investigators. The APT team are the deepest technicians, and they understand viruses and attacks and malware and every acronym I can throw out there. They also have deep connections to the outside. They spend a lot of time talking with APT types in other companies and government agencies. They look at the outside world, to help us predict what *might* happen, more than at what's going on in our network.

Novartis has created a similar organization; Bancroft pointed out that the people required to staff it are somewhat unusual:

> Some things benefit from centralization. Security is probably one of them. Our incident management is run by specialist people who know what to do, who know what the rules

> are. Specialists are expensive people, because these are guys who potentially could make more money on the outside, being the bad guys. They are *massively* technical.

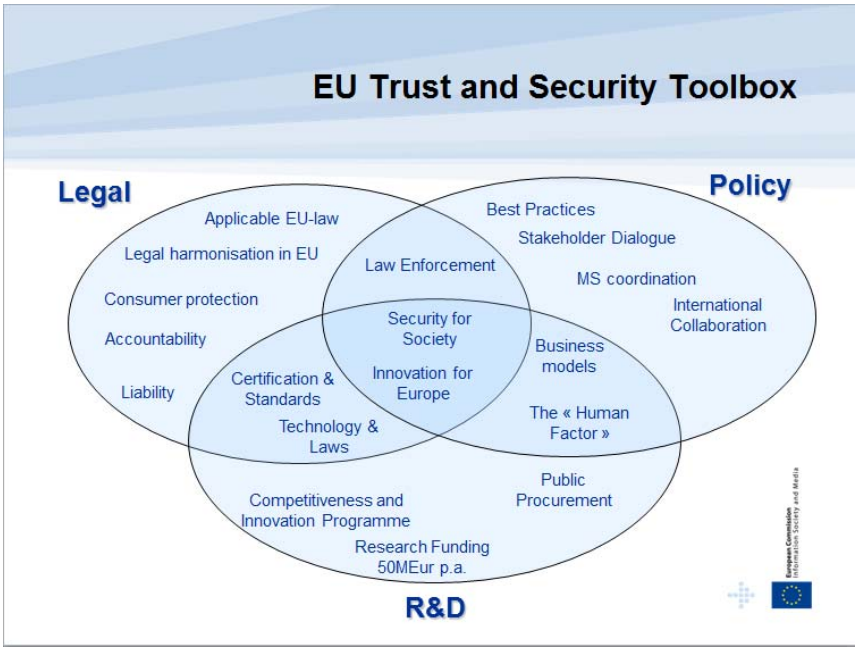
Martino's description of Cisco's APT team led to the question of collaboration. Bancroft made the point that "It's often the same people attacking everybody's company. But we all basically stop at our firewall, and it's left to law enforcement, which is hopelessly overworked, under-resourced, and under-funded, and can't reach across international borders."

ING's Diemont suggested that the Netherlands may be taking good first steps, with its national cybercrime center. "It is a public-private partnership with police, justice, and high-tech crime units. Is that enough for us? It's good that it's happening, but we are not losing money in the Netherlands to crime, it's going across borders. We should force our governments to really push on this, to work together, to work internationally. Otherwise we will lose the battle."

Cisco's Martino offered a different emphasis: "One thing the government can do is <u>not</u> get into the technology. They tend to do some of that — like where my data is stored. I'm not sure that actually helps us operationalize or protect our data in any greater fashion. If government stayed focused on international law and international enforcement, and not so much in the technology, I think would help the private sector. There's a role for the government to play in technology and innovation, right, but day-to-day operations is not a place for them."

Martin Mühleck is a Project Officer in the Trust and Security Unit of the European Commission. In a presentation he gave to the group, he described both some of the complexities and some of the opportunities associated with cross-border collaboration in cyber-security:

"The strong instrument that governments have is legal/regulatory, which is not very popular," Mühleck said. "When we see other problems, developing a solution can take years, and either the problem has solved itself, which is the optimistic version, or the solution of yesterday is no longer



useful. So more and more, the European Commission and the European Institutes are careful of putting too much regulation and legislation in the field of security.

"There are examples," Mühleck continued,

> Where partnerships are actually in place and are working and are promising in their results. Botnets are a good example, because there's good understanding and wide support. With the help of ENISA, we are building up the EP3R — the European public-private partnership for resilience. The first two years were spent very much on bringing people together, creating a basis for trust and mutual understanding of where collaboration is possible and necessary. Now we can say with confidence that we have a group that wants to work together, and is going to produce concrete results. On a general level, European initiatives can bring the following added-value: If you have a security problem in your country, and you see that you cannot deal with it alone, be need support in a neighboring country, the first step is to know the structures: Who is the right person to call in the neighboring country? Who is the person who knows and understands the relevant structures and how they work? So it's no longer at the personal level. EU CERT and other CERTS will intensify that collaboration through and beyond ENISA. Law enforcement is getting on board (see the new European Cyber Crime Centre). They are all interested in creating structures for better integration of different stakeholders and how information can be better shared. Trust between individuals is easy. Building trust between organizations and state member groups, especially if they work in different ways, in a different area — that's much more difficult. We must work on that, and we must improve on that.

Bancroft from Novartis remained unconvinced:

> So these future EU data protection directives are interpreted differently in every country, and national policies take precedence over it. So although it's there, if it's interpreted differently in different cultures or if national laws take precedence, then it's a moot point. It's massively frustrating that these guys can keep coming back and attacking me and I can do almost nothing about it, because they're in Russia or somewhere else. Do the law enforcement people plan to ever ask for help? Because I'd be happy to provide resource, provide expertise, consultancy, whatever it is, because if we wipe out one, it benefits everybody.

Godfrey from Goldman Sachs supported the concept of industry-government cooperation:

> There are certain jobs that only the authorities can do, and so we spent the past couple of years working at how we, as an industry, share information, collaborate on information, and create that information exchange structure. The government security sources sit on top of it and receive the information, but we aren't dependent on them doing anything with the information. They're busy. But it would be nice to have the authorities a bit more purposed and focused on solving the things that we can't solve from the law enforcement angle, figuring out how to do law enforcement across jurisdictions, because those are things that are wholly outside our control.

Cisco's Martino suggested that there are ways to foster the industry/government partnership:

> In the US, the military has seconded employees to my organization for six months or a year. I don't pay them, but they work for us. They do what I ask them to do, and we train them in our processes and our techniques, and they go back better-equipped to help the military do what they need to do for themselves.

Parting Shots

It's a tradition at CDS workshops to ask each participant for a summary thought on the day. Nokia's Boije observed both the commonality and the difficulty of cyber-security: "There are as many approaches to security as there are participants. We still face the same challenges, but there are no silver bullets." Hilti's Gourinchas expressed one of the major themes: "The new threats with mobile apps and elsewhere makes it very hard. We need to come back to the human factor; awareness is key here, and we should not give up. Let people collaborate; we're just trying to inform them, so that they can moderate themselves."

Simic from Swarovski agreed: "Collaboration is key for future information security development, to organize our strategy and our missions." Brechbühl from CDS took a different perspective, and questioned what it would really take for the "good guys" to ever defeat the "bad guys:" "I see an ever-increasing need to pay attention to things that are longer-term and insidious in nature and that you may not even know are there — the kind of campaign that may start very silently and stay silent for a long time, perpetrated by the types of organizations that have a lot more patience than any of us do."

Enrico Senger of Schindler brought the conversation back to where it had started, the first and last purpose of information security:

> I see the challenges that we all discussed, and at the moment we separate business from security, but in the end, all of the security problems arise because business is trying to get new opportunities. I liked the statement that security should enable business, and I think this is a direction that will become more and more important, especially with all the new technology and consumerization and so on. We need to try, at least, to steer in that direction, to address the value of what was discussed here, to develop more opportunities for business in the future.

Participant List

Cybersecurity: Risks, Mitigation and Collaboration

An Executive Workshop for European CISOs

20 June 2012

Scott Bancroft	Group CISO Novartis International AG
Johan Boije	Director, Security & Continuity Capability Area Nokia
Hans Brechbühl	Executive Director Center for Digital Strategies Tuck School of Business, Dartmouth College
Mark Connelly	CISO Thomson Reuters
Ton Diemont	CISO ING
Nick Godfrey	Head of EMEA Technology Risk Goldman Sachs
Olivier Gourinchas	Head of Market Reach, Service Management and IT Security Hilti
Markus Hänsli	Vice Director, Federal Office of Information Technology, Systems and Telecommunication FOITT Swiss Confederation
M. Eric Johnson	Benjamin Ames Kimball Professor of the Science of Administration Director, Center for Digital Strategies Tuck School of Business, Dartmouth College
Peter J. Kunz	Manager Infrastructure Security Information Technology Management, Global Information Security Daimler

Yvon Le Roux	VP, Cyber Security Cisco
Steve Martino	VP, Information Security Cisco
Amal Mezzour	Global Information Security Officer Holcim
Jeffrey Moore	Sr. Enterprise Security Manager Adidas
Martin Mühleck	Project Officer DG INFSO Unit F.5 Trust and Security European Commission
Josef Nelissen	CISO ABB
Boris Otto	Assistant Professor & Head of Competence Center Corporate Data Quality Institute of Information Management University of St. Gallen
John Petersen	IS/IT Security Manager Nestlé
Enrico Senger	Head IT Strategy & Transformation Schindler Informatik AG
Martin Sibler	VP, Risk Management - Information Security Swiss Reinsurance Company Ltd
Valentin Simic	Corporate Information Security Manager Swarovski
Gérald Vernez	Deputy Director, Cyber Defense Project Federal Department of Defense Swiss Confederation