Deloitte.

The Value of Cyber Risk Quantification

October 13th 2016
Maastoren, Rotterdam

The impact of cyber-crime is not limited to individual companies. Through interdependencies, a cyber-attack may cause knock-on effects with potentially devastating consequences.

Supported by the World Economic Forum, Deloitte has been working with company boardrooms to improve our understanding of cyber risk. This includes answering questions like: How big is cyber risk exactly? What do we need to do to mitigate this risk? When is it sufficient? To answer these questions in a meaningful way, cyber risk quantification through Value-at-Risk approaches have been developed. So far, these remain limited to individual organizations.

"This calls for dialogue", says Maarten van Wieren, Senior Manager Cyber Risk Quantification at Deloitte and host of this event. "Exchanging information, suggestions and solutions. Like learning to ride a bicycle, risk management is about finding the balance between risk and opportunity.

"Risk management is about finding the balance between risk and opportunity."

Maarten van Wieren

Given the complexity of cyber risks, it's not easy to determine where this balance lies. It's a bit like stumbling in the dark. This seminar will inspire discussion on the purpose and potential of cyber risk quantification for society as a whole and help turn on the lights."

The importance of quantified information

Risk assessment is important; how else can you effectively invest in cyber security?, according to Patricia Zorko, Deputy National Coordinator for Security and Counterterrorism and Director Cyber Security at the National Cyber Security Centre (NCSC). It should be a joint effort, but not everyone seems to be convinced of the computational approach. Moreover, terrorism is often considered a bigger risk, while the risks of becoming a victim of cyber-crime are much bigger. The financial impact of cyber-crime can be huge as well: it costs billions of euros. We need to prove this, Zorko states. All the more reason to get the data in order. And there's another thing: two out of three companies that are hacked or spied on, don't know they are hacked or spied on. Others are afraid to tell or don't think it's significant. So there's a lot of work to be done, and NCSC's Dutch awareness campaign Alert Online is part of this.

This year's Cyber Security Assessment Netherlands contains 4 significant developments, explains Wouter Oosterbaan, Cyber Security Advisor at the NCSC. Professional criminals are evolving into more advanced actors carrying out long-lasting and high-quality operations. They operate in an advanced fashion and in large teams. **Digital economic espionage**, stealing intellectual property or products in development and possibly bringing it to another country, puts a strain on the competitiveness of The Netherlands. Even though espionage is happening on a daily basis, most companies are unaware of it. The third development, **malvertising**, entails infecting consumers with malware by infecting ads and banners on websites. Advertising networks have not yet shown the ability to cope with it. Lastly, the goal of **ransomware** is to infect as many people as possible through phishing and spear phishing, encrypt their data and demand money for undoing this. This form of cyber-crime is commonplace and becoming more advanced, with increasing profits. It's the go-to business model and will not go away.

Both Zorko and Oosterbaan stress the importance of quantified information, though obtaining data is not easy. It's hard to put a number on the loss of competitiveness of a country, but it's a necessity for accurate assessments. That's why NCSC keeps developing frameworks and dashboards and publishing reports. Furthermore, public-private cooperation nationally and internationally is the core of our Dutch approach and can help obtaining more data. Therefore, we should not compete on cyber but strengthen public-private partnerships.

The upside of cyber risk

With more open and connected technology, it is inevitable that we face increased cyber threats an vulnerabilities. Organizations are well aware of this. Now it's tempting for security consultants to paint a Digital Armageddon, instill fear and say: hire me. But fear is the wrong approach, says 'cyber libertarian' Roel van Rijsewijk, senior fellow with Deloitte's

Center for the Edge and author of *Cyberrisico als kans*. Fear has a function, but if it takes over and we are led by fear, we are doomed.

We live in a transformational time, the dawn of the information age. Most historians agree there are three fundamental shifts in human evolution driven by technology; the agricultural revolution, the industrial revolution and – as we are now witnessing – the third revolution, the information revolution. And everything will change fundamentally, it's going very fast and nobody knows what the future will look like, not even Google or Apple. We are faced with complete uncertainty.

You can fear uncertainty. Realize that the fight against hackers is an asymmetric fight (they only need one tiny hole in an ever evolving IT landscape) and you do not know that they will come up with tomorrow.

What Van Rijsewijk suggests is that companies should of course take appropriate security measures and be compliant, but not only focus on the downside of cyber risk. Because if they do, they will adopt a 'cover your ass' strategy that consists of ticking all the boxes and produces a lot of policies and procedures. It's 'digging in', leading to paper-based compliance and a control system (bureaucracy) that tends to expand. You're like a knight in shining armor who fell of his horse: very vulnerable.

Total security is not only impossible, it's undesirable as well, states Van Rijsewijk. Instead of locking your data down, you should utilize it. Share it, don't protect it. Connect, empower your organization, trust your people, create user centric IT and more transparency. In short, create value connected technology and the free flow of information. What's the use of Rembrandt's Night Watch if it's kept in a vault?

And with creating value, you create cyber risk. And this is the upside of cyber risk: if you manage the related risks better, you can innovate faster, get more value out of data and put more empowerment in your organization. Not by being secure but by being resilient against cyber-

"Total security is not only impossible, it's undesirable as well."

Roel van Rijsewijk

attacks. Keep security to an absolute minimum and be open and connected and then detect threats in a timely manner so you can respond effectively. By being vigilant you can quickly detect, respond, learn and recover to a higher level.

Where do those numbers come from?

Cyber risk quantification is the desired thing. But all estimates in dollars or euros are speculative, says Michel van Eeten, full professor at Delft University of Technology and member of the Dutch Cyber Security Council. Reasonable conjecture at best. That's why is so hard for organizations to calibrate optimal levels of cyber security investments.

A case in point is the EU project called E-Crime. After having established that the estimates were fictional, the researchers had to reframe the problem of impact and come up with another framework. A framework that was qualitative – built on interviews with IT experts – but very insightful.

What's wrong with current cyber risk estimates? Well, it's just not clear where the numbers – those billions of dollars – come from. How they are attained. What data makes McAfee state that cyber-crime costs US society 400 billion dollars per year? Most of such estimates are derived from open data like country numbers, which are based on numbers of research organizations, which are based on specialized reports about IP losses, which eventually lean on 'expert opinion'. It's like opening Russian dolls to find that the last one is empty. In other words: we don't have a clue. How can we quantify Intellectual Property losses? If you are a pharmaceutical company and your R&D is stolen, the actual damage is pretty hard to assess. There's going to be a cheap med on the grey market, but that would happen anyway, also without a cyber breach. The protection against this is intellectual property law. So trademark protection is more relevant than cyber security.

Measuring the economic impact of cyber-crime is complicated. There are two basic categories. First, there is wealth transfer. It is not 'wealth loss', because the money travels from one firm to the other. It didn't go to Mars, but stays in the economy. Second, there's opportunity costs in terms of anticipation of the cyber incident, the consequence of it and the response to it. Some say the real damage is not the money lost but the eroding of trust, leading to customer avoidance and reduced adaption of innovations. Van Eeten, who says he is suffering from a 'bias' called empiricism, cannot find hard data that shows this erosion of trust.

"Productivity losses is what we have to look at."

Michel van Eeten

Even opportunity costs in the Health industry are not exact, because, for example in The Netherlands, hospitals had no obligation to report incidents and estimates are based on extrapolations. How to monetize these losses, then? It's challenging, but worth the effort. You can quickly see that the cost of protection – cyber security measures and their effects on productivity – far outweigh the out-of-pocket losses of a data breach. So it's not cyber-crime itself, but the response to it that costs most money. That's why we shouldn't focus on out-of-pocket losses, says Van Eeten. Productivity losses is what we have to look at.

Dilemmas, voting & discussion

Cyber risks are not typically limited to the firms directly impacted, consumers and third parties may also get impacted. As was identified in World Economic Forum report, a "tragedy of the commons scenario is emerging […], which lacks concerted controls and safeguards". Organization of concerted efforts is the domain of public-private partnerships and the dilemma comes down to choosing between two approaches that both have their own distinct drawbacks. On the one extreme top-down policies and regulations can be imposed, while self-organizing coordination could emerge on the other extreme. We tested the sentiment on this dilemma with the audience as well as with the speakers presenting them with three multiple-choice questions.

Dilemma 1

Suppose a large firm is failing because it had its vital data compromised. Its suppliers and customers also suffer the consequences. Other examples of third party risk include outage of critical infrastructure or compromise of a security firm. What level of attention should managing third party risks receive from companies?

A. Not to worry, 3rd party risk is not too large and we have everything under control.
B. Although 3rd party risk is large in some cases, it is mostly under control.
C. We are underestimating 3rd party risk and we need to increase our efforts.
D. 3rd party risk leads to significant systemic risks and concerted efforts are needed.

The majority in the room votes for C (52%). Patricia Zorko states it's important to control and minimize systemic risks, irrespective of who they're from. Roel van Rijsewijk is struggling: in a situation where everybody is dependent on everybody, no one is responsible. On the other hand, a distributed network is extremely resilient because there is no more 'one point of failure' where data can be stolen. So the more mutual dependency, the more resilience.

Dilemma 2

In public-private partnerships, what is the best strategy to assign these responsibilities?

A. It is the full responsibility of asset owners to ensure proper risk mitigation with legislation to protect against abuse.
B. Asset owners are primarily responsible but should receive support from the government in identifying and addressing abuse.
C. Asset owners and government should collectively address the risks with private parties in the lead.
D. The government should identify and control a "public part of cyber space" including capabilities to protect.

Most votes in the room go to C (41%). Patricia prefers B but tends to choose A also: asset owners have a responsibility. Roel: "As a cyber libertarian I say: with great freedom comes great responsibility. So regulate yourself before you get regulated." But since cyber-crime is physically located in countries, governments should take measures? Governments have a role to play, replies Roel, but it is a very small one. "Living in

"The value of cyber risk quantification in all of this is obtaining the key insights needed to balance the risk and reward from cyber, for individual organizations and society alike."

Maarten van Wieren

Amsterdam and riding my bicycle there, I see lots of traffic regulations. Now, some managers have had the balls to refrain from regulation and, in some areas, let traffic regulate itself. This hands-off philosophy seems to work. Chaos works."

Dilemma 3
Increased coordination and sharing of data through the public sector is necessary in order to enable concerted cyber security measures.

A. No, through sharing cyber risk data, we actually create additional risks, this is better handled privately.
B. The current infrastructure for sharing information through the NCSC is sufficient.
C. We need more macroscopic data also relating to economic impact through a common taxonomy with help of e.g. CBS, CPB etc.
D. The government should establish trusted authentication and provide transparency and data sharing for a "public part of cyberspace".

The large majority in the room votes for C (65%). Michel rejects A and D and finds B and C to be mutually exclusive. He votes for C. Roel: "We should strive for full transparency, which is partly a government responsibility. A cyber breach is not a shameful thing. Share it and learn from it. There's an enormous leap we can make. If we want transparency, we need to be less restrictive and find a better balance between freedom and punishment. Mistakes happen." Patricia indicates that the policy strives for B while the challenge is realizing C and D could definitively help with that.

Concluding remarks

Balancing the role of private enterprise and government has always been a challenge. Now, especially in the face of common threats in the form of

complex and highly unpredictable cyber risk, this challenge is even harder. As we gain and share insights into cyber risk as a society, we greatly improve chances to make the right decisions and maintain cyber space as a common good and avoid a tragedy of the commons.

In this debate, a couple of main points stand out:

1. Cyber threats aren't limited to individual organizations and the threat of unpredictable spill-over effects with catastrophic consequences is real.

2. The precise nature and potential magnitude of these spill-over effects is unknown because cascading effects may aggravate an incident.

3. Because of this uncertainty, organizational agility and flexibility in dealing with incidents.

4. In addition, we need to improve our understanding and coordination efforts as a society regarding potential cyber catastrophes.

5. Achieving these goals will have the highest chance of success through joint public-private efforts.

The value of cyber risk quantification in all of this is obtaining the key insights needed to balance the risk and reward from cyber, for individual organizations and society alike. Based on the survey held during the meeting, the general opinion emerges that the government should take a leading role with such efforts as data collection and defining a common taxonomy. Through investing in measuring and quantifying cyber risk, efficient and effective management of cyber risk is enabled, not only for individual organizations, but also for society as a whole. Only in this way, can we expect to collectively limit cyber risks to a level needed to maintain the emerging benefits of technology.

Maarten van Wieren
Deloitte Netherlands
Tel: +31 (0)88 288 7139
Mobile: +31 (0) 6 8201 9225
Email: MvanWieren@deloitte.nl

Vincent Lukkien
Deloitte Netherlands
Tel: +31 (0)88 288 6674
Mobile: +31 (0)6 1371 2154
Email: VLukkien@deloitte.nl

Vivian Jacobs
Deloitte Netherlands
Tel: +31 (0)88 288 3376
Mobile: +31 (0)6 2015 7774
Email: VJacobs@deloitte.nl