Audit Committee News
Edition 56 / Q1 2017 / Risk Management & Compliance

Addressing cyber risks in an increasingly connected world

Introduction

Media reports on cyber incidents are everywhere these days. According to the Global Risks Report 2016 published by the World Economic Forum (WEF) such crimes in cyberspace cost the global economy an estimated US $445 billion, more than many economies' national incomes.

In KPMG's 2016 Global CEO Outlook, cyber security climbed the list to become the top risk over the next 3 years. At the same time 72 percent of the CEO's indicated they feel not fully prepared for a cyber event.

Local examples in the past year that have had a major impact on businesses, either with a reputation or economic impact, are a large-scale cyber-attack that focused on Swiss online shops and a high-profile data exfiltration at a Swiss corporation. Although the nature of these incidents and the type of attackers are most likely not comparable, it leaves the general impression that nothing connected to the internet is safe anymore. This last statement is not true and this article is intended to provide insights on what companies can do to actively manage cyber risks.

It is not all about technology

Whereas cybercrime has a strong connotation with "technology", fighting it effectively requires an integrated and balanced approach involving both people and processes as well as technologies. A study of the University of St. Gallen shows that companies which have a competent responsible person for cyber risks are less often victims of a cyber-attack.

Whilst cyber security is on top of many board agendas, companies struggle to properly assess, measure and communicate to what extent their business is resilient against cyber-attacks. This understanding is paramount in order to tackle cyber risk effectively.

It is not recommended to simply invest in all potential areas or outsource the problem completely to a provider. This should be a diligent decision after assessing a company's specific risk profile. There are a number of questions which can help to focus the discussion about cyber security within a company:

- Who would be potential attackers interested in attacking the company? There is a vast array of criminal motivations, like cyber espionage, organized crime or hacktivists, who all operate differently and will be creating a different type of damage.
- How much sensitive data (health records, credit card numbers, etc.) do you hold within your responsibility? Here it is important to know what types of data you have, where they are stored, how they are being secured. This includes classifying your data and knowing what is sensitive or not, technical measures for safeguarding but also educating employees to deal with data in a sensible way.
- How much reliance is there on third party providers for your infrastructure? Next to traditional outsourcing the interconnectivity between systems of different companies is continuously increasing. Knowing where the boundaries are and including cyber risk components in contracts and service level agreements are key for managing these relationships proactively. This is also applicable to equipment through which employees can connect themselves to the organization in the context of "bring your own device".
- Do you operate or make profit in a controversial industry? For each specific sector there is a different risk profile. Especially hacktivists can focus on controversial industries while these sectors can be less interesting for organized crime.
- How much do you trust your own employees of not making mistakes (deliberately or not)? Many of the incidents that happen around cyber risk have a beginning which is on the inside of an organization and involves employees. The traditional actor is a disgruntled employee who abuses his/her rights to cause damage. In other instances, like the "Fake President" cases, employees are simply tricked in conducting certain actions in a scheme they do not comprehend. Raising awareness, educating employees and making them alert as part of the defense mechanism will make a difference.
- How many of your products contain an "Internet of Things" component? In case your new products are equipped with some form of connectivity it is no longer about only securing your own organization but also about taking responsibility for your customers. How do you ensure your product is not being abused and becoming part of some criminal scheme? In October a large distributed denial of service (DDoS) attack was executed mostly by leveraging internet connected devices such as HD recorders, cable set-top boxes, routers and even Internet-connected cameras. Companies whose products get new connectivity components will need to include cyber security into their design processes.

There are many more questions that could be addressed than the ones above. There is no standard fixed list and, once answered completely, one is cyber security safe. When it comes to cyber security the ability to continuously learn and adapt is more valuable than just being compliant with a set of standards.

A simplified model to assess potential measures to help reducing the cyber risks is shown below.

Cybercrime defense framework

	Prevent	Detect	Respond
People	• Risk awareness and technology understanding training (threats, vulnerabilities and impact) • Corporate attitude programs (e.g. conscious learning mode programs)	• Security operations center	• Crisis organisation • Communications
Processes	• Compliance monitoring • Vulnerability monitoring • Security testing • Patch management • Incident preparedness training	• Incident monitoring • Emergency hotline	• Attack mitigation procedures • High-value asset isolation procedures
Technology	• Segmentation • Endpoint and perimeter protection • Security baselines	• Logging and alarming • Incident dashboards	• Data collection and preservation • Forensic analysis • Data recovery

Residual risks

Even if all the measures above have been considered and implemented there is still no guarantee that everything will be 100 percent safe. Here we can make the parallel to how we deal with the risk of fire impacting a business.

What happens in a company if a fire breaks out? Smoke detectors go off, the sprinkler system is triggered and employees call the fire brigade. However in some situations even these preventive measures cannot help anymore. In such situations fire insurance mitigates the company's financial damage. These insights can be applied to cyber risks as well. Managing cyber risks by implementing protection measures and control systems is crucial for every company. But in certain situations, only cyber insurance can alleviate the financial damage of a cyber-attack. The insurers financially support the firms to analyze the actions of the hackers, to plug leaks and recover data. Depending on the policy they even insure for damage to customers and provide legal staff and cybercrime experts.

From reactive to predictive

Given the strategic relevance of cyber security, a reactive approach to managing the cyber risk is no longer sustainable. New regulations in place or coming soon, like Guidelines for Operational Risk (FINMA 2008/21) or the EU General Data Protection Regulation (GDPR), present an ideal momentum to develop an insight-based, risk-focused and predictive management of cyber risk. For example, the GDPR will drastically increase the fines to be paid in case of a failure to protect private data of customers or employees.

The GDPR comes into play in 2017 and the enforcement is expected to start in May 2018. It still has to be clarified how the ruling will be upon failing to report a data breach in a timely manner but it is for sure that if a proper process and activities around mitigation of cyber risk can be shown to the regulators, this will have a positive influence on the level of potential fines.

Looking forward

The dynamics of cyber security will change as the interconnectedness of the world accelerates in the turn towards complete connectivity. It is evident that part of our longstanding technology and processes can no longer keep up. The blurring lines between physical, digital and biological spheres create new security challenges in spaces like Internet of Things, Industry 4.0, etc. Mastering these challenges, having a proactive approach and integrating security in the design of processes and products will be the license to do business in the future. Integrating cyber security in the core of your business can be the competitive differentiator in a world that thrives around trust between parties and keeping clients (and client data) safe.

Gerben Schreurs
Forensic, KPMG AG
gschreurs@kpmg.com

Matthias Bossardt
IT Advisory, KPMG AG
mbossardt@kpmg.com