How to be prepared for cyber attacks

A solution based approach

Everyone who has been following the news knows how organizations are struggling with their cyber security. Files in organizations and institutions all around the world have been encrypted until ransomware demands are paid. If you are an IT Security Manager, HSSE Manager, or play any role in security and risk management for any type of company that uses an IT infrastructure, you will be or have been facing the dangers of cyber risk. While your current risk management tools may have worked in the past regarding security issues, it is plausible to ask if they suffice to manage the cyber risks of today and the future. By the end of this white paper, we hope to have painted the landscape of cyber risk and its implications and answered the question about the risk management methods and tools that are necessary to navigate the world of cyber security.

Worldwide cyber-attacks continue to increase

Over the past decade, cyber security incidents have frequently made headline news. On May 12th, 2017, the digital world is hit by the ransomware WannaCry. Files in organizations and institutions all around the world were encrypted. The only way to recover them was to pay a ransom. As organizations are increasingly relying on IT systems, they become more vulnerable to cyber-attacks like WannaCry.

Another recent example is the worldwide Petya ransomware attack that took place in June of 2017. With this ransomware attack, hackers were able to shut down the operations of multiple organizations at once. One of the largest container shippers in the world, APM terminals, saw 76 of their port terminals shut down for weeks, which cost up to $300 million. Potential downtime of operations, and/or permanent loss of sensitive data pose a dangerous and potentially costly threat to organizations.

If you are an IT Security Manager, HSSE Manager, or play any role in security and risk management for any type of company that uses an IT infrastructure, you will be or have been facing the dangers of cyber risk. Increasing interconnectivity, globalization and "commercialization" of cybercrime are driving greater frequency and severity of cyber incidents.

While your current risk management tools may have worked in the past regarding security issues, it is plausible to ask if they suffice to manage the cyber risks of today and the future. The complex and abstract field of cyber security may seem vastly different from physical security at first, but other than some superficial differences, you will find many similarities with older branches of security and risk management.

By the end of this white paper, we hope to have painted the landscape of cyber risk and its implications and answered the question about the risk management methods and tools that are necessary to navigate the world of cyber security.

The complexity of the problem

Cyber security risks include hackers stealing sensitive data, or influencing critical processes. In the past stealing was a physical act, so organizations could focus on physical protection of their products and assets from thieves. Nowadays, organizations rely on digital sources much more and have integrated IT in their day to day operations and management systems.

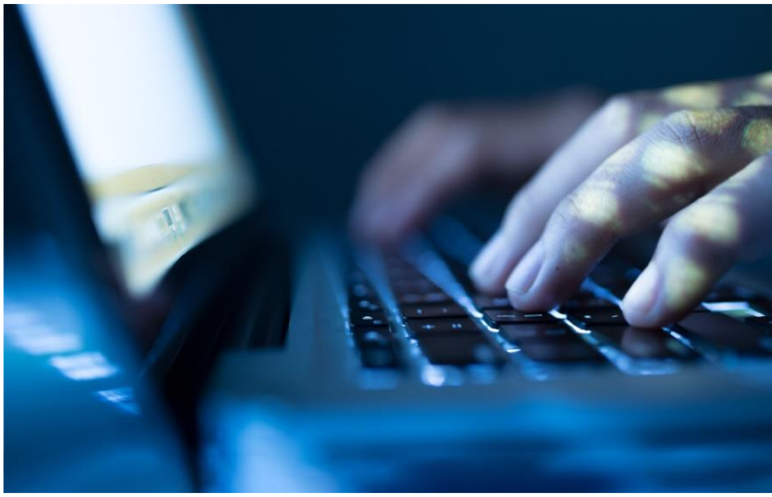
In addition to security issues, safety issues arise as soon as cyber security breaches affect operational equipment. Take for example GPS systems of vessels, airliners and other transportation devices, where hostile take-over or jamming could result in a collision with possibly catastrophic consequences. Vulnerability of industrial control systems (ICS) to attack poses a significant threat. To date there have been accounts of centrifuges and power plants being manipulated by the infamous Stuxnet worm. However, the damage could be much higher from security sensitive facilities such as nuclear power plants, laboratories, water suppliers or large hospitals (Collins, 2015).

Cyber-attacks like WannaCry and Petya do not seem to target specific organization or users, but seek the path of least resistance and trust to reach their goals by targeting numerous organizations at once. In the WannaCry example, this was possible because many organizations are still reliant on old, unsupported software like Windows XP, which has not received public security updates for half a decade, and even those that are running on newer operating systems are often sporadically maintained (Hern & Gibbs, 2017). On the other hand, cyber criminals are investing in the future and are continuously looking for ways to improve, just as your own organization is doing. It is up to your organization to set up safeguards or 'barriers' to protect your data and the assets against the cyber-attacks.

The typical end goals of cyber-attacks are to steal and exploit sensitive data and to affect the operation by influencing critical processes. However, that is not everything security and risk professionals have to think about. In addition to the actual risks for your IT, assets, reputation and operational continuity there is the development of governmental awareness of cyber threats and the accompanying legal implications. Complying with new legislation is an important factor that cannot the overlooked.

Laws and directives

The first country in the world to implement laws and not directives concerning protecting critical infrastructure were the United Arab Emirates (UAE). This was inspired by computer infections in the Middle East increasing at a rate above the global average. To boost their national cyber-security capabilities and elevate the protection level of critical national information infrastructures, they have stepped up their cybersecurity activities in recent years.



The UAE were not alone in acknowledging the increased cyber risks and the need for action. The European Commission announces the following on their website:

'In January 2012, the European Commission proposed a comprehensive reform of data protection rules in the EU. [...] EU Member

States have to transpose it into their national law by 6 May 2018.

The objective of this new set of rules is to give citizens back control over of their personal data, and to simplify the regulatory environment for business. The data protection reform is a key enabler of the Digital Single Market which the Commission has prioritized. The reform will allow European citizens and businesses to fully benefit from the digital economy (European Commission, 2011).'

To comply with the EU directive and soon to be effective European General Data Protection Regulation (GDPR), The Netherlands already enforced the Bill on Notification of data leaks (Dutch Data Protection Authority, 2015). The Bill introduces the duty for data controllers in the Netherlands to notify a breach of security measures protecting personal data to the Dutch Data Protection Authority. In addition, fines for violations of the Dutch Data Protection Act will significantly increase. Failure to comply with the rules may lead to fines of up to € 810,000 or 10% of the organization net annual turnover.

GDPR implications for risk management

The regulation (European Commission, 2016) specifically and repeatedly refers to proper risk assessment (Data Protection Impact Assessments), safeguards and the legal implications of non-compliance to these standards.

Article 35 requires organizations to perform Data Protection Impact Assessments to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed. Paragraph 84 mentions the controller is responsible for carrying-out a risk assessment for high-risk operations and taking into account the outcome to determine appropriate safety measures. Furthermore, paragraph 148 specifically states that the height of an administrative fine in case of infringement of the regulation is partly influenced by the safeguards in place and actions to mitigate the damage suffered.

Paragraph 90 summarizes the impact for risk management professionals:

"In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation."

The European General Data Protection Regulation (GDPR) also calls for the mandatory appointment of a Data Protection Officer (DPO) for any organization that processes or stores large amounts of personal data, whether for employees, individuals outside the organization, or both. DPOs must be:

"Appointed for all public authorities, and where the core activities of the controller or the processor involve 'regular and systematic monitoring of data subjects on a large scale' or where the entity conducts large-scale processing of 'special categories of personal data,'" (European Commission, 2016).

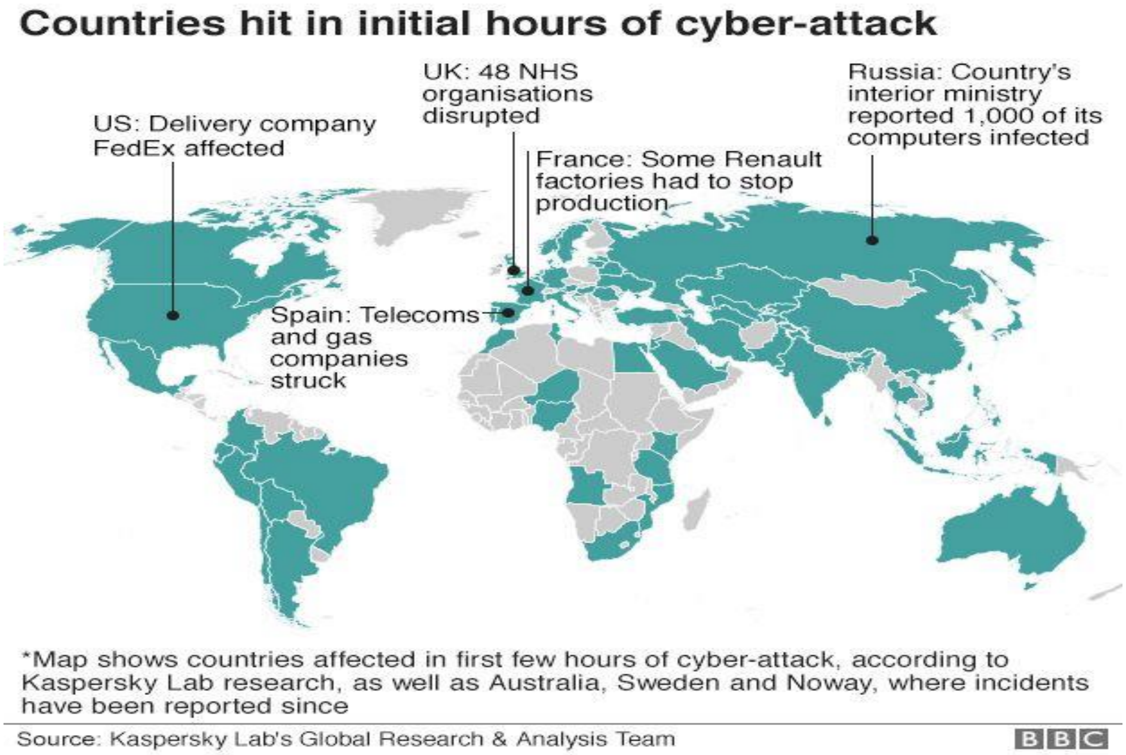
The DPO oversees all data protection activities within an organization. They will be the first point of contact for data protection issues within the workplace. It is a key advisory role, providing guidance on the identification and management of privacy risks. Important duties are conducting risk assessments, implementing a data security risk management strategy and communicating about these risks to the rest of the organization. This leaves the DPO with a set of responsibilities that seem to require proper risk management skills and tools to fulfill the goals of the Regulation.

In conclusion, there are two main reasons to improve cyber security risk management. First, the actual threats to the organization's sensitive data and operations, and second, the new legal implications and subsequent potential financial penalties.

Cyber and physical security: a different approach?

Cyber security is a new challenge for organizations, but does it also require a new approach to deal with that challenge? Let us compare cyber and physical security. Firewalls and virus scanners are in a way the digital equivalent to gates and security guards. But what makes cyber security different?

First, the scale and speed of cyber-attacks is much larger. It is common for attacks to span multiple countries or continents in a day. For instance, WannaCry spread to at least 99 countries infecting more than 75,000 computers in a day.



Countries hit in initial hours of cyber-attack

US: Delivery company FedEx affected

UK: 48 NHS organisations disrupted

France: Some Renault factories had to stop production

Russia: Country's interior ministry reported 1,000 of its computers infected

Spain: Telecoms and gas companies struck

*Map shows countries affected in first few hours of cyber-attack, according to Kaspersky Lab research, as well as Australia, Sweden and Noway, where incidents have been reported since

Source: Kaspersky Lab's Global Research & Analysis Team

Figure 1: http://www.bbc.com/news/world-europe-39907965

Second, the rate of change is higher. Of course, physical security is also constantly evolving, but over the past decades, the rate of change in the IT security sector has been increasing. WannaCry used an exploit that was discovered, fixed and exploited in the course of two months. Because many organizations had not applied the fix yet, the virus could spread as wide as it did. The rapid rate at which new risks emerge and holes in existing 'barriers' are exploited creates a new challenge.

Third, the dependencies on external software and libraries is much larger. For example, the Heartbleed bug in 2014, where a security bug in the OpenSSL library compromised many systems that relied on the encryption it provided. It can be argued that physical security also depends on services from external contractors, but the dependencies in IT tend to be more extensive and dynamic.

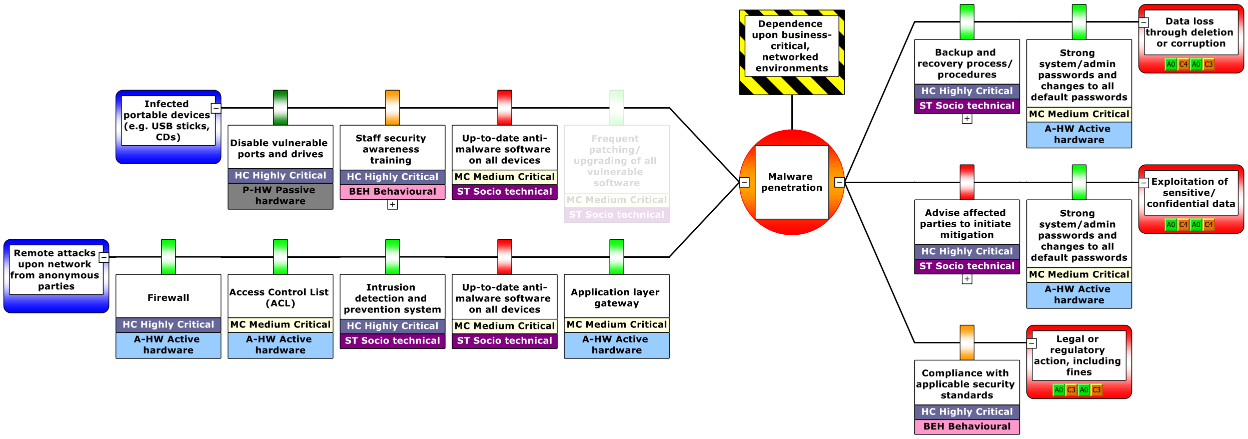
Fourth, it can be difficult to detect certain types of cyberattack. A machine can be infected for extended periods of time without any detection. This is less likely with physical security.

The question remains whether these differences warrant a new approach. The answer is, partly. A lot of the concepts that are applied in the real world also hold true in the digital world. There are risk scenarios that need to be identified, and control measures need to be put in place to prevent those scenarios from unfolding. The next section Visualize cyber security will cover how existing methods can be used for cyber security. To contrast that, the section on Accelerated Continuous improvement will discuss how the existing methods need to be adapted to deal with the unique challenges of cyber security.

Visualize cyber security

Conventional risk assessments are mostly conducted in an Excel environment. However, risk assessments have the tendency to become very complex and abstract making it difficult to understand for non-experts.

The bowtie methodology translates Excel fields with plain text about risks and barriers into easy to interpret risk scenarios. Visualizing the risk assessment through the bowtie methodology has the advantage to make it easier for non-experts to understand abstract risks and provides experts a structure to share knowledge.


Dependence upon business-critical, networked environments
Infected portable devices (e.g. USB sticks, CDs)
Disable vulnerable ports and drives
HC Highly Critical
P-HW Passive hardware
Staff security awareness training
HC Highly Critical
BEH Behavioural
Up-to-date anti-malware software on all devices
MC Medium Critical
ST Socio technical
Frequent patching/ upgrading of all vulnerable software
MC Medium Critical
ST Socio technical
Remote attacks upon network from anonymous parties
Firewall
HC Highly Critical
A-HW Active hardware
Access Control List (ACL)
MC Medium Critical
A-HW Active hardware
Intrusion detection and prevention system
HC Highly Critical
ST Socio technical
Up-to-date anti-malware software on all devices
MC Medium Critical
ST Socio technical
Application layer gateway
MC Medium Critical
A-HW Active hardware
Malware penetration
Backup and recovery process/ procedures
HC Highly Critical
ST Socio technical
Strong system/admin passwords and changes to all default passwords
MC Medium Critical
A-HW Active hardware
Data loss through deletion or corruption
A0 C4 A0 C3
Advise affected parties to initiate mitigation
HC Highly Critical
ST Socio technical
Strong system/admin passwords and changes to all default passwords
MC Medium Critical
A-HW Active hardware
Exploitation of sensitive/ confidential data
A0 C4 A0 C4
Compliance with applicable security standards
HC Highly Critical
BEH Behavioural
Legal or regulatory action, including fines
A0 C3 A0 C3

The diagram above is a cropped part of a full cyber risk bowtie that has 'Malware penetration' as the top-event, which is the loss of control moment of the hazardous activity. It shows two threat lines on the left side, and three consequence lines on the right. The barriers in between are assessed by their effectiveness with the colored flags, and have their criticality and barrier type attached beneath the barrier box. Of course, these are just examples of information that can be displayed on the diagram.

Because the 'infected portable devices' threat line has only one highly effective barrier and two poor ones, we want to implement a fourth barrier which is greyed-out in the example. Furthermore, we see that the consequence 'Legal or regulatory action' consequence has only one barrier and thus seems highly exposed. This could indicate that the single barrier is a highly critical one and therefore deserves our full attention to be properly maintained.

Looking at the barrier type classification, it shows that the 'security awareness training' is a behavioral barrier, highlighting that IT security is not merely a technical affair. It can be insightful to see the barrier type distribution in the context of all related bowtie information, to highlight any weak spots or possible common failure modes. In another example where the IT manager is responsible for 90% of the barriers, this could cause problems if he is ill or not functioning well. Bowtie diagrams provide such insight.

In short, the bowtie diagram visualizes risk and helps making complex and abstract matters understandable, gives overview, grants new insights and facilitates easier communication to all stakeholders.

Accelerated continuous improvement

As shown, the bowtie method enables organizations to analyze existing risks and the status of existing barriers. It is possible to use the method for continuous improvement, but this process is usually spread out over multiple months or years. Companies are used to plan their risk management improvement cycles by their own account.

Cyber security is different because the type of attacks keeps changing and evolving at an incredible rate. The need for improvements and updates is dictated by third-party influences in the form of software releases, updates, patches, vulnerability alerts, and of course the ever lurking cyber criminals and their efforts.

This requires organizations to respond faster to these new threats. This high pace changes the way continuous improvement is done. Basically, an accelerated continuous improvement process is needed to cope with the quickly evolving and changing landscape of cyber threats. The bowtie method as a tool is only powerful if an organization acknowledges that cyber-attacks require a change of mind and a change of pace.

We can perfect our risk identification and analysis, but there will always be ‘unknown unknowns’ – the ones we don't know we don't know. Moreover, if we look throughout the history of cyber security, this category tends to be the difficult one and inflicts the most damage.

References

Collins, S. (2015, September). *White paper: Cyber Risk Guide.* From Allianz: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/cyber-risk-guide/

Dutch Data Protection Authority. (2015, 12 8). From Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/policy_rules_data_breach_notification_obligation.pdf

European Commission. (2011, 1 18). *Protection of personal data: European Commission*. From European Commission: http://ec.europa.eu/justice/data-protection/

European Commission. (2016, 4 27). *European Commission.* From Data protection: European Commission: http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

European Commission. (2016, 12 13). *Guidelines on Data Protection Officers ('DPOs'): European Commission.* From European Commission: http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf

Hern, A., & Gibbs, S. (2017, 5 12). *tech: The Guardian*. From The Guardian: https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20