Information Security Risk Management

François Thill

Information Security Risk Management

François Thill

Ministère de l'Économie, Luxembourg, Luxembourg
francois.thill@eco.etat.lu

Abstract. Behavioural security, technical security and organisational security are inter-related. Issues addressing security should therefore consider those three pillars in common not in silos.
This paper summarizes a keynote speech held on this topic at the 16th IFIP Summer School on Privacy and Identity Management.

Keywords: Information security, risk management, cybersecurity, informed governance.

1 Introduction

Behavioural security [1], technical security and organisational security are inter-related. Issues addressing security should therefore consider those three pillars in common, not in silos, as it is often the case.
In 2020, 84% of cyberattacks relied on social engineering [2], and studies show that implementing solely technical measures without involving and educating users is futile [1]. Organisational security is about increasing the efficiency of both behavioural and technical security by defining clear security targets, assessing risks, defining responsibilities and allocating resources effectively to treat these risks.

2 Technical Cybersecurity

Technical cybersecurity is the implementation, configuration, and maintenance of technical security measures, such as anti-virus, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS).
So-called *signature-based tools* rely heavily on the accuracy as well as on the timeliness of the data they use to recognize and stop threats. These technical security tools mostly implement proprietary standards. Customers using this type of technical security tools have to buy the appliance, the product license, and subscribe to costly information feeds updating the search patterns of these tools.

Skilled cyber criminals try to obfuscate [3] their attacks and adopt evasive measures to prevent automatic detection and mitigation of their attacks. This adaptive behaviour from the side of threat actors has decreased efficiency of proprietary cybersecurity tools and pushed companies to implement threat-hunting activities. This process is complex and ties up many skilled cybersecurity resources (forensic and threat

hunting). Especially if consumed as a service from an external Security Operations Centre (SOC), it can become very expensive [4]. Due to the scarcity of human resources[1], cybersecurity reveals as discriminatory in terms of costs and complexity.

3 Technical Cybersecurity is a Data Economy

Technical cybersecurity represents a data economy. Thanks to initiatives like the Malware Information Sharing Platform (MISP[2]), this data economy is slowly evolving from a data oligopoly to an open economy.

Data sets used in this data economy are for instance Indicators of Compromise also called "forensic artefacts of an intrusion that can be identified on a host or network" [5], their sightings, the sectors they are found in. There are of course many more data sets existing, including information about threat actors, vulnerabilities, efficiency of protective and reactive measures.

Standard commercial tools are no longer able to effectively and automatically counter threats (see previous chapter) pushing many companies to start threat hunting. This development, combined with the activities of the Computer Emergency Response Teams, is fostering a more open data economy in technical cybersecurity.

Some actors, especially governmental ones, continue to share their information only under the "need to know principle", providing vital cybersecurity information only to a few actors, thereby leaving others unprotected.

According to the ENISA study [6], threat intelligence is currently in the early adoption phase compared to incident response and security operations practices. Threat information, representing the raw material for threat intel, is data laboriously gathered by collecting, storing and analysing logs (network, end-point, firewall, Intrusion Detection Systems, ...), as well as investigating low level security alerts to reclassify them if necessary and start an investigation to gather Indicators of Compromise (IOC). This redundant investigation done by company experts or third party experts (external Security Operations Centre SOC) into "low signals", potentially revealing malicious activities within their company or constituency networks, hide a huge synergy potential. Due to the scarcity of human resources in cybersecurity, these synergies should be capitalised through a more open data economy, allowing the continuous and timely exchange of threat indicators.

Especially in Europe, this has led to the creation of threat exchange platforms, where experts from SOC or Computer Emergency Response Teams share their findings such as indicators of compromise, forensic analysis, and context information.

One of the best-known initiatives is the Malware Information Sharing Platform (MISP). Like any data economy, this threat information economy needs to address data governance issues with regards to technical, semantical and legal interoperability of the data they share. It also has to comply with the European legislation on data exchange platforms[3] and most likely also on AI[4].

---

1 https://go.globalknowledge.com/2020salaryreport

2 https://www.misp-project.org/

3 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767

Technical and semantical interoperability issues are solved by defining cross-sectoral taxonomies. Legal interoperability is achieved by implementing legal requirements (secondary use, pseudonymisation, anonymization) coming for the General Data Protection Regulation[5] or from sectorial regulations such as banking[6] or health.

4 Organisational Security

Technical security is highly dependent on high quality data in terms of accuracy and timeliness. If technical security measures rely on biased, incomplete or outdated threat intelligence, their efficiency is directly affected and negative impacts may follow quickly.

This *direct causal link* between the accuracy of cybersecurity data and the effectiveness of measures is less obvious in organisational security. Erroneous decisions in organisational security might take some time to spread their harmful impact.

Risk assessment, "the overall process of risk identification, risk analysis and risk evaluation" [7] is required by both standards, such as the information security management standard ISO/IEC27001 and legal frameworks, such as Network and Information Security Directive[7] or the General Data Protection Regulation[8].

Many companies are required to implement a risk assessment process and feed the results into the internal governance process, as well as report its outcome to regulators. **Risk assessment is an integral part of governance, on company, corporate, national and European level**.

The Information Security Management Standard ISO/IEC 27001 requires that "repeated information security risk assessments produce **consistent**, **valid** and **comparable results"**. This general requirement applies not only to governance but also to **regulation**.

In organisational cybersecurity, the risk assessment process is most dependent on accurate data. **As mentioned above, the usage of biased, incorrect or incomplete data in organisational cybersecurity does not immediately create a visible impact. Reasons for incidents are most often sought after in the technical cybersecurity domain. The governance decisions that led to the configuration of these tools are rarely questioned.**

---

4 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

5 https://www.misp-project.org/compliance/gdpr/information_sharing_and_cooperation_gdpr.html

6 https://www.circl.lu/services/misp-financial-sector/

7 https://op.europa.eu/en/publication-detail/-/publication/d2912aca-4d75-11e6-89bd-01aa75ed71a1/language-en

8 https://eur-lex.europa.eu/eli/reg/2016/679/oj

5 Organisational Cybersecurity Needs to Become a Data Economy

The breath-taking evolution of cybersecurity threats, especially due to the professionalization of threat actors [8], has dramatically changed the way to address organisational cybersecurity as a company and as a country respectively within the European Single Market. Information about modus of operandi of threats, the appearance of catalysing technologies such as crypto currencies[9], or the discovery of new vulnerabilities[10] have to be collected to enrich the situational awareness of companies and the regulators. Obviously, this information also has to be cast into new risk scenarios during the risk identification phase.

Furthermore, threats and vulnerabilities have to be qualified respectively quantified. Their probabilities respectively ease of exploitation are changing over time and have to be adapted during the risk evaluation phase of the risk assessment process.

While the usage of this data is quite common in technical cybersecurity, **its valorisation in organization cybersecurity is not.** This data is however crucial for the realisation of a consistent and valid risk assessment process.

6 Creating the Data for Organisational Situational Awareness

As organisational cybersecurity will become an open data economy, data governance principles need to be developed to foster the creation of technically, semantically and legally interoperable datasets.

Contributors of these datasets are multiple:

- Computer Incident Response teams contributing with information about incidents (scenarios), threats, their probabilities, vulnerabilities, their ease of exploitations and effectiveness of risk treatment measures;
- Regulators with information about minimum scope of risk assessments, context information, impact thresholds, risk acceptance information, incidents (national and international);
- Security Operation Centres with information similar to threats;
- Security researchers;
- Research done with techniques known in finance [9].

The ISO/IEC 31000 standard [7] states "that risk assessment should be conducted systematically, iteratively and **collaboratively**, drawing on the knowledge and views of stakeholders[11]" fostering collaboration.

---

[9] Some cyber-criminal business-cases could only materialize with the help of crypto-currencies

[10] For instance, company networks opened to the Internet to allow for teleworking during the Covid-19 pandemic, leading to process and technical vulnerabilities.

[11] Stakeholder is defined in the standard ISO/IEC 31000 as "person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity."

The Luxembourg government is conscious about the challenges this requirement of the ISO/IEC 31000 poses and is convinced about the importance of this approach. For this reason, the Luxembourg government will invest, in the context of the IPCEI-CIS[12], in the creation of a **cybersecurity data space** in the spirit of the European strategy on data[13], aligned with the Luxembourg Data-Driven Innovation Strategy [10] and the Strategy "Ons Wirtschaft vu Muer" [11]. It will be made available and accessible just like the other Common European Data Spaces[14].

Based on the cybersecurity data space, risk management information such as common and sectoral risk scenarios, risk estimation information such as threat probabilities, ease of exploitation of vulnerabilities will be made available broadly.

The Cybersecurity Competence Centre of SECURITYMADEIN.LU made very promising work in transforming technical cybersecurity information into risk information by mapping cybersecurity incidents via the Mitre Att@ck[15] to risk scenarios.

7 Towards an Informed Governance

Sharing risk information such as scenarios, threat probabilities, ease of exploitation of vulnerabilities is unproblematic from the point of view of the GDPR or other sectorial regulations. Sharing this information is of utmost importance [12], because risk managers generally have a hard time identifying relevant risk scenarios and even more problems qualifying respectively quantifying risks. Without accurate and objective information, risk management is futile and ends-up in a completely subjective exercise producing random results. This is especially true for small companies. They represent the vast majority of European companies, are often strategic actors in large' supply chains and play a key role in building inclusive and resilient societies [13]. For this reason, SMEs often handle highly critical data containing trade secrets, intellectual property rights or private data.

Regulators or cybersecurity agencies providing community-wide and objective risk information, based on factual information, will not only improve the quality of individual risk management. Thanks to the introduction of common risk taxonomies, risk management will become comparable, repeatable and reliable throughout the community. Only by achieving this level of collaboration and coordination, **risk management will become a governance tool instead of being a compliance exercise.**

Luxembourg has announced in its national cybersecurity strategy III [14] that the concepts of informed governance (risk management based on common taxonomies and collaborative situational awareness) will be developed. The creation of the cybersecurity data-space and the research done on the level of transforming technical cybersecurity information into organisational cybersecurity information brings Luxembourg a step closer to this goal. Sectorial regulation in cybersecurity (GDPR, Bank-

[12] https://www.bmwi.de/Redaktion/EN/Artikel/Industry/ipcei-cis.html
[13] https://digital-strategy.ec.europa.eu/en/policies/strategy-data
[14] http://dataspaces.info/common-european-data-spaces/#page-content
[15] https://attack.mitre.org/

ing, NIS, Critical Infrastructure Protection, …) can be partially harmonised and the price of regulation can be reduced while increasing its efficiency dramatically.

References

1. ENISA: *Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity*, 2019. https://www.enisa.europa.eu/publications/cybersecurity-culture-guidelines-behavioural-aspects-of-cybersecurity
2. ENISA: *Threat Landscape 2020 – Main Incidents*, 2020. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-main-incidents
3. ENISA: *Threat Landscape 2015*, 2016. https://www.enisa.europa.eu/publications/etl2015
4. ENISA: *Proactive detection – Good practices gap analysis recommendations*, 2020. https://www.enisa.europa.eu/publications/proactive-detection-good-practices-gap-analysis-recommendations
5. OpenIOC: *Sophisticated Indicators for the Modern Threat Landscape: An Introduction to OpenIOC*, 2017.
6. ENISA: *Exploring the opportunities and limitations of current Threat Intelligence Platforms*, 2018. https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms
7. ISO: *ISO 31000:2018 Risk management — Guidelines*, 2018
8. Europol: *Internet Organised Crime Threat Assessment (IOCTA)*, 2020. https://www.europol.europa.eu/publications-events/main-reports/iocta-report
9. Michel Verlaine: *On the extraction of cyber risks from structured products*, Applied Economics, 2021. DOI: 10.1080/00036846.2021.1998327
10. The Luxembourg Government – Ministry of the Economy: *The Data-Driven Innovation Strategy for the Development of a Trusted and Sustainable Economy in Luxembourg*, 2019. https://gouvernement.lu/en/publications/rapport-etude-analyse/minist-economie/intelligence-artificielle/data-driven-innovation.html
11. The Luxembourg Government – Ministry of the Economy: *Ons Wirtschaft vu muer – Roadmap for a competitive and sustainable economy 2025*, 2021. https://meco.gouvernement.lu/en/publications/strategie/strategie-ons-wirtschaft.html
12. OECD: *Digital Security Risk Management for Economic and Social Prosperity - OECD Recommendation and Companion Document*, 2015. https://www.oecd.org/sti/ieconomy/digital-security-risk-management.htm
13. OECD: *OECD Studies on SMEs and Entrepreneurship: The Digital Transformation of SMEs*, 2021. https://www.oecd.org/publications/the-digital-transformation-of-smes-bdb9256a-en.htm
14. The Luxembourg Government – High Commission for National Protection: *Stratégie nationale en matière de cybersécurité III*, 2018. https://hcpn.gouvernement.lu/en/publications/strategie-nationale-cybersecurite-3/strategie-nationale-cybersecurite-3/strategie-nationale-cybersecurite-3.html