DOI: 10.26314/GARR-Conf22-proceedings 19

Sustainability of cybersecurity for ME&SMEs

Enrico Frumento, Andrea Guerini

Cefriel Politecnico di Milano (IT)

Abstract. The COVID-19 pandemic was an accelerator in the digital transformation agenda of many businesses and a discontinuity in how cybercrime operates. More recently, the Ukraine-Russia conflict added the geopolitical driver to the logic of cybercrime. As a result, keeping an organisation secure became a complex process. Cybersecurity is nowadays a problem of sustainability more than technologies. Sustainable cybersecurity means a readily available and rapid method to understand the value of exposed assets from a cybercriminals point of view, assess the status, calculate the cyber-risk and the economic impacts of cyberattacks and coherently, cost-wise plan the mitigations from multiple perspectives. Especially micro, small and mid-size enterprises (ME&SME) need sustainable cybersecurity

Keywords. cybersecurity sustainability, cyber risk, cyber risk appetite

Introduction

The Digital with a Purpose (Digital with a Purpose, 2022) is a movement of "leaders joining forces in a race to deliver against the Paris Agreement and Sustainable Development Goals by 2030 [...] to create a sustainable world through responsible, ICT-enabled transformation", which follows the launch of their 2019 report (GeSi, 2019). The report identifies and quantifies how digital technologies can help accelerate efforts to achieve seventeen identified sustainable development goals. However, despite cybersecurity not being directly listed, there is no better aim while going digital than to secure your operation and business sustainably. Sustainability in cybersecurity is not directly connected to the environment but refers to broader sustainability concepts concerning technologies, the human element and costs. This means keeping estimated cyber risks under control through sustainable and applicable mitigations.

1. Cyber risks for ME&SMEs

ICT companies are frequently the first adopters of new technologies and thus must ensure they implement exemplary cyber security safeguards into their business practices and services. ME&SMEs must consider the always challeng-ing balance between cyber risks, affordable mitigations, operational capability, and costs. The smaller the organisation, the more difficult is this compromise. The post-COVID-19 years and the Russian-Ukraine conflict changed the deci-sional landscape, and cyber-risks for ME&SMEs are increasing for three main reasons.

1. The pervasiveness and the reliance on digital technology of almost all prod-ucts, services and processes. The digital technologies, characterised by high-speed innovation, high-

growth rates and substantial market potential, power the ongoing digital (r)evolution. This revolution affects large compa-nies, who generally have sufficient resources, start-up and ME&SMEs, which are the most delicate and essential backbone of the EU economy and usually do not have enough resources or competencies in cybersecurity.

2. A new wave of disruptive technological and economic changes accelerated by the recent COVID-19 pandemic and the conflict between Russia and Ukraine. These two factors represent a discontinuity in cybercrime and cy-bersecurity through renewed Tactics, Technologies, and Procedures. ME&SMEs accelerated digital transformation, even for the more conserva-tive sectors, heavily affected cybersecurity. As a result, cybercrime is in "overdrive" (K. Teal, 2020). ME&SMEs are in focus, and a further attacks in-crease is highly likely (Robert Walters, 2020).

3. Investment in cybersecurity dilemma. ME&SMEs more than even balance the pros and cons of cybersecurity investments, redefining their "appetite" for cyber-risks, often on dangerous assumptions. A recent survey (ISSA, 2020) reports that while 25 per cent of ME&SMEs think their organisations will be forced to decrease security spending for 2021, 30 per cent say cy-bersecurity will be a higher priority.

ME&SMEs are under economic pressure, forced to adopt a rapid digital transformation agenda operating in a weak economic context and, more than before, highly targeted by cybercriminals (Vu, 2020). Therefore, ME&SMEs need to consider efficient and sustainable defence strategies and optimise their forces and expenditures to minimise the risk of being ruined by a cyberattack.

2. What does "sustainable" mean in the fight against cybercrime?

Sustainable cybersecurity for ME&SMEs means a readily available and rapid method to understand the value of their tangible and intangible assets from a cybercriminals point of view, assess the existing status, calculate the cyber risk and the direct and indirect economic impacts of cyberattacks and coherently, cost-wise plan the mitigations from multiple perspectives. In other words, treat cybersecurity as a business decision (Proctor, 2020). All these operations are being done considering ME&SMEs' time, preparedness, and operational capaci-ty. However, ME&SMEs are very heterogeneous, and solutions must be tailored to different levels of expertise and requirements. Smaller organisations need practical guidelines and technical solutions, while more oversized need prod-ucts and standards. A primary one-stop shop providing lightweight procedures and advice would be beneficial as a starting point for planning a sustainable cy-bersecurity journey. Sustainability also means comprehensibility. The Cyberse-curity Act (European Parliament, 2019) lays down a framework for establishing EU cybersecurity certification schemes to ensure an adequate level of cyberse-curity for ICT in the EU and avoid the internal market fragmentation. The Act states that ICT services and processes must "improve their cybersecurity risk management activities by improving, for example, users' cybersecurity vulnerability management and remediation procedures" and underlines the importance of measuring and mitigating cyber risk. However, ME&SMEs find themselves in trouble when assessing and managing cyber-risks. Due to the complexity of the problem, the scar-

city of human and financial resources, and the lack of risk management attitudes require a specific and novel approach.

3. Gaps in ME&SMEs cyber-resilience

Nowadays, cybercriminals must be considered stakeholders of the digital trans-formation agendas: they follow their agenda of doing business with the same assets of law-abiding companies but with very different business plans. Despite budget constraints and a lack of time and knowledge, cyber-security is usually not a fundamental issue in the ME&SMEs agendas, focusing instead on competi-tiveness driven by a short time to market and cost minimisation. This makes ME&SMEs' capability of reaction and recovery generally low (Privacy Australia, 2019). These organisations often have relatively inadequate IT security prepar-edness and do not fully see the (even long-term) consequences of being a victim of a cyber-attack. We refer here, for example, to the cascading long-lasting economic and operational consequences in case of tangible and intangible as-sets loss. The problem of increasing cyber resilience for ME&SMEs is complex and made of two elements. First, the ME&SMEs landscape is diverse, with varie-ties in size, sector, geography, technological intensity, and markets served. Sec-ond, ME&SMEs can be (potential) users and suppliers of emerging and not still secure technologies. Currently, already more than 90% of EU ME&SMEs consid-er themselves lagging in digital innovation (European Commission, 2018), also because of uncertainties and gaps in the protection of their assets and lack of required skills (EISMEA, 2022). Moreover, as reported (Asti, 2019), despite con-flicting statistics, "small and medium businesses may be being targeted more fre-quently, and the cyber-attacks may be taking more time to resolve, presenting an urgent challenge to the cyber defence of small and medium businesses".

The problem of increasing cyber resilience for ME&SMEs is complex because of:

- Usually, low preparedness in cybersecurity and not always dedicated and/or sufficient resources and budget for it.
- In Europe, most ME&SMEs are members of either someone else's supply chain as a supplier/contractor or an ecosystem. Therefore, their cybersecu-rity posture influences someone else's cyber risk (Help Net Security, 2019).
- ME&SMEs are often merged/acquired, and this implies also acquiring their cyber-posture. A recent survey highlights that "53% of IT and business deci-sion-makers report their organisation has encountered a critical cybersecurity issue or incident during a Mergers and Acquisitions deal" (Help Net Security, 2019).
- Their decision workflow is generally short, and the decisions takers (CTO, CFO, CISO etc.) are a handful of people; roles might overlap or even collapse in a single person (Javaid, M et al., 2017);
- Management and training of human resources are essential, e.g., reskilling for ME&SMEs (Capgemini Invent, 2019)).
- Intangible assets are very relevant, e.g., reputation for ME&SMEs that are part of a supply chain.
- The cyber risk acceptance logic is not always "be secure". Sometimes the decision is

to remain vulnerable to avoid business interruptions, and loss of competition limits investments without a clear and specific return (Javaid, M et al., 2017).

- Work-as-done vs work-as-prescribed issue: in ME&SMEs, what is in the field often does not entirely correspond to what is documented. Therefore, current maturity models (e.g., ISO or CC) are not wholly mapping what is concretely operative and on the field (Lisanti, Y. et al., 2017).

4. Sustainable cybersecurity

There is not a direct correlation between the energetic consumption of an IT in-frastructure and its security. Therefore, more sustainable cybersecurity means something else. The sustainability of cybersecurity is not represented in ener-gy-intensive terms: instead, it is described in technological, economic, pro-cess, human and necessary knowledge. This concept implies a holistic ap-proach, estimating the total cost of ownership of cybersecurity (see Figure 1). To estimate these total costs, ME&SMEs require a tailored cyber-risk manage-ment solution (e.g., each supply chain has its cyber-risk logic) that is trustable and explainable.

- Trustability of cyber-risk estimations. Organisations do not trust the risks as they are presented and worry about putting their finite resources in the wrong places.
- Explainability of cyber-risk. Many implicit knowledge and assumptions are involved in standard cyber-risk assessments leading to less effective deci-sion-making.

Some additional research is required in this area to propose a sustainable ap-proach. Something also initiated by the European project HERMENEUT (E.Frumento et al., 2019). In general, the fundamental needs are:

- Quickly determine an organisation's cyber-posture and detect precursors of emerging threats.
- Provide an explicit knowledge and valuation of the tangible and intangible assets at cyber risk.
- Identify the position of the organisation in the specific supply chain/ecosystem and the possible cascading effects on the other members of the supply chain/ecosystem.
- Offer an agile, affordable, and simplified approach to cyber-risk man-agement and decision-making to minimise the existing ME&SMEs cyber-knowledge gaps while also considering budget limits.
- Adapt to cyber-risk acceptance logics arising from being part of a supply chain/ecosystem.

5. Conclusions

The pandemic and the ongoing conflict forced digital transformation and influ-enced supply chains. The digital transformation agenda suddenly accelerated with severe implications on cybersecurity and cyber-risk exposure and the for-mer supply chains (H. Mudassir, 2020). This acceleration urges "shorter" (fewer actors, more closely tied and less geographically distributed) and resilient (composed by trusted peers) chains. The consequent general weakness of ME&SMEs worsened the problem of cybercrime sustainability: less

money, be-sides an increased cyber risk, creates a dangerous short circuit between the willingness to take risks, balancing the potential losses with the immediate re-mediation costs. In parallel recent prosecution and closure of mainstream groups and underground forums forced cybercrime to become insular and to challenge to probe (M. R. Fuentes, 2020). For these reasons, the sustainability of cybersecurity is a critical issue.

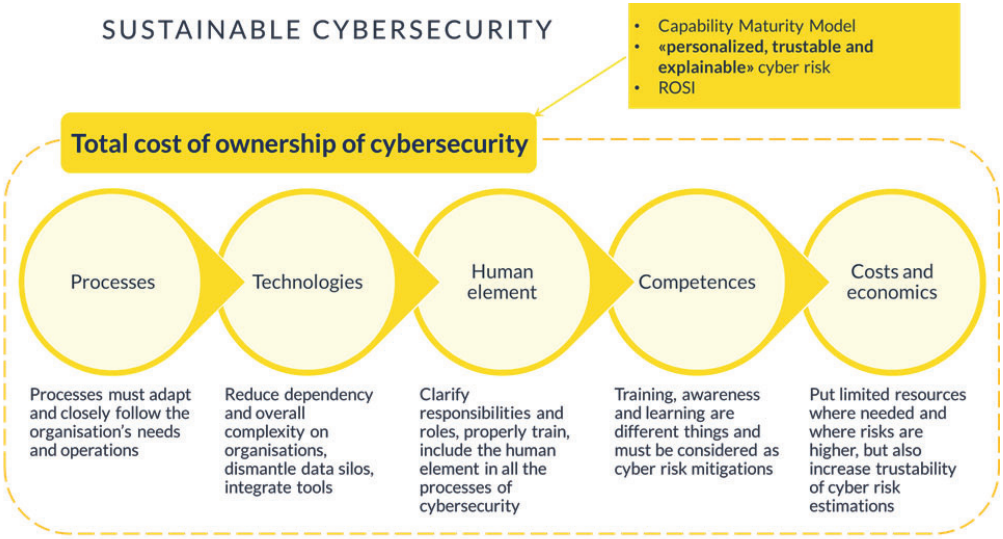

Fig. 1
The total cost of ownership in cybersecurity comprises five pillars or areas where the costs are shaped.

Bibliography

Asti, A. (2019). Cyber Defense Challenges from the Small and Medium-Sized Business Perspective. SANS Institute Information Security Reading Room.

Capgemini Invent. (2019). Skills for SME Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity for SMEs. European commission.

Digital with a Purpose. (2022). Retrieved from https://digitalwithpurpose.org/

E.Frumento et al. (2019). The role of intangible assets in the modern cyber threat landscape: the HERMENEUT Project. European Cybersecurity Journal, 5(1), 56-64.

EISMEA. (2022). Retrieved from European Innovation Council and SMEs Executive Agency: https://eismea.ec.europa.eu/index_en

European Commission. (2018). Capitalising on the benefits of the 4th Industrial Revolution. Retrieved from https://data.europa.eu/doi/10.2777/588385

European Parliament. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 52.

GeSi. (2019). Digital with Purpose: Delivering a SMARTer2030. Retrieved from https://gesi.org/research/download/36

H. Mudassir. (2020, 3 16). COVID-19 Will Fuel the Next Wave of Innovation. Retrieved from https://tinyurl.com/w355z2t

Help Net Security. (2019, June 25). How much risk small businesses really pose to supply chain cybersecurity? Retrieved from https://tinyurl.com/25pbu3b9
Help Net Security. (2019, June 25). You don't just acquire a company, but also its cybersecurity posture. Retrieved from https://tinyurl.com/2bznpk6n
ISSA. (2020, August). The COVID-19 pandemic and its impact on cybersecurity. Retrieved from https://tinyurl.com/2a4alex3
Javaid, M et al. (2017). A comprehensive people, process and technology (PPT) application model for Information Systems (IS) risk management in small/medium enterprises (SME). International Conference on Communication Technologies (ComTech).
K. Teal. (2020, June 1). 'Cybercrime Tactics and Techniques': COVID-19 Sends Attackers Into Overdrive. (Channel Futures) Retrieved from https://tinyurl.com/25q6p7yo
Lisanti, Y. et al. (2017). IT service and risk management implementation for online startup SME: Case study : Online startup SME in Jakarta. International Conference on Information Management and Technology (ICIMTech).
M. R. Fuentes. (2020). Shifts in Underground Markets (Past, Present and Future). Trend Micro.
Privacy Australia. (2019). [Report] Most Common Vulnerabilities for SMEs (2015-2019).
Proctor, P. (2020). The Urgency to Treat Cybersecurity as a Business Decision . Gartner.
Robert Walters. (2020, August 18). CYBERSECURITY: BUILDING BUSINESS RESIELENCE. Retrieved from Robert Walters: https://tinyurl.com/29pdknw4
Vu, A. V. (2020, July 14). The Effect of the Coronavirus Pandemic on aCybercrime Market: A Stimulation. (Cambridge Cybercrime Centre) Retrieved from https://tinyurl.com/28nqn3rg

Authors

Enrico Frumento enrico.frumento@cefriel.com

Dr Enrico Frumento is a Senior Domain Specialist in the cybersecurity team at Cefriel. He is the author of subject-related publications and books and a member of the European CyberSecurity Organisation and the European Digital SME Alliance. His 20+ years of research focus on unconventional security, cybercrime intelligence, a contrast to modern social engineering and dynamic assessment of organisations' vulnerabilities corresponding to tangible and intangible assets at risk.

Andrea Guerini andrea.guerini@cefriel.com

Dr Andrea Guerini is a Researcher and Consultant in Cybersecurity at Cefriel. With a multidisciplinary education focusing first on communication and then on IT security, he concluded his studies with a postgraduate degree in Strategic Protection of the Country System at SIOI in Rome. His activity at Cefriel is mainly focused on innovation and learning projects and, in particular, on the importance of the human element in cybersecurity processes, supporting decision-makers through analysis, storytelling and data visualisation and executing assessments aimed at measuring cyber risk.