Cybersecurity risk management: How to strengthen resilience and adapt in 2021

Insights and recommendations from research and innovations projects and entities

2021

Acknowledgements

Cyberwatching.eu is grateful to the projects and individual experts that have contributed to the series of webinars of the project clusters on the topic of cybersecurity risk management, and to the recommendations provided in this document. More details and contact details can be found in section 6.

Contents

1 Cybersecurity risk management: How to strengthen and adapt in 2021

Cybersecurity risk management has become a priority for companies and organisations. Staying ahead of threats and regulatory compliance is no joke, let alone how to identify risks, prioritise and take action. So, what steps can you take to ensure resilience and build trust in your services?

Cyber risk management can be challenging in multiple ways given that many organisations do not perceive the risk until something bad happens and many smaller organisations do not have the means or even the awareness of the risks that exist. All too often, an SME (or even a large company or organisation) only sees their risk exposure when an actual breach occurs, a denial-of-service attack or when they are "locked out" of their own data by a ransomware attack.

This 17th webinar entitled "Cybersecurity risk management: How to strengthen resilience and adapt in 2021"[1], gathering over 132 registered participants from 29 countries around the globe.

The webinar focussed on standardisation and certification, in particular in relation to the large European SME community with presentations from ECSO[2], which provided a policy setting to the webinar and key players such as SGS[3], and Cyberwatching.eu partners Digital SME Alliance[4] and AON[5].

The webinar also shone the light on R&I research into the topic. Six R&I projects CyberSure[6], CUREX[7], GEIGER[8], PANACEA[9], RESISTO[10] and SECONDO[11], presented their research in the field highlighting the risk management challenge they address, the key results and the main impacts of these results on European organisations (in particular SMEs).

A key aspect of the webinar was to highlight the importance of online resources and tools which target SMEs. These are essential in helping SMEs prepare for cyberattacks and become more resilient. The Cyberwatching.eu Risk Management tool and the forthcoming cybersecurity certification seal, are tools that can help organisations to expose and employ prevention mechanisms in areas where there could be significant cybersecurity risks, which were not identified and addressed previously.

[1] https://cyberwatching.eu/cybersecurity-risk-management-how-strengthen-resilience-and-adapt-2021
[2] https://ecs-org.eu/
[3] https://www.sgsgroup.it/
[4] https://cyberwatching.eu/european-digital-sme-alliance
[5] https://cyberwatching.eu/aon
[6] https://cyberwatching.eu/projects/1789/cybersure
[7] https://cyberwatching.eu/projects/1814/curex
[8] https://cyberwatching.eu/projects/2126/geiger
[9] https://cyberwatching.eu/projects/1270/panacea
[10] https://cyberwatching.eu/projects/1974/resisto
[11] https://cyberwatching.eu/projects/1972/secondo

2 Helping SMEs understand the value of certification

2.1 Why a lightweight cybersecurity label is the way forward for SMEs

Website: www.sgsgroup.it
Contributor: Lucio Gonzales-Jimenez[12]
CyberLab Madrid Manager

SGS has been a testing, inspection and certification company since 1878, with a strong commitment to the cybersecurity domain.

Implementing processes, procedures and policies to protect information and data is essential for all companies. And these challenges are faced in every single sector, **no matter specialization or company size.** Certification is very important because it helps you to protect your **business** (market differentiation, supply chain, etc.) and **customers** (security by design, etc.). In addition, the EC launched the **Security Industry Policy** in 2012 that underlined the importance of meeting standards and certifications to overcome market fragmentation.

Currently, the certification ecosystem (certification, accreditation, audits, etc.) is a very **complex environment from the SME point of view**. There is a strong need to offer SMEs a clear approach to help them understand what they have to do to avoid getting lost during the process. The **EU Cybersecurity Act** and the different certification schemes that are to be implemented will help, but this is still a long road and a lot of information to read and process.

Taking into account the amount of information regarding schemes, standards and methodologies that an SME needs to understand to properly choose the testing, inspection and certification services to improve its position in the market, it's highly recommended, as a first step, to trust in a **consulting firm** to help SMEs to implement the standards and/or technical certifications. The second recommended step is an internal exercise of **self-assessment** to identify the critical assets you want to protect. The third and final step is the **certification** itself, accredited by a Third Independent Party. These three steps are as important as **different** to be competitive in the Digital Single Market (for instance, in some countries you need to be certified in order to sell your products to public administrations).

In spring 2021 the **SME Cybersecurity Label** will be launched. Created by SGS and the Cyberwatching.eu project the label is designed to ease the entrance of SMEs into the certification ecosystem. The label provides a **self-assessment based on a robust approach and a solid background to the certification path**.

Recommendations from SGS

More online resources should be made available to the SME community. The Cybersecurity Label

[12] https://cyberwatching.eu/lucio gonzález-jiménez

will provide SMEs with an accessible first step to understanding the areas in which they have gaps in security and the types of actions that they should take towards an eventual certification. Covering topics such as software, protocols, hardware and infrastructure, the label provides a first check for SMEs in helping them to understand, evaluate and assess security gaps. This lowers the barrier to entry into the certification process and gets companies into the habit of carrying out checks of systems which can lead to greater resilience and ultimately trust for their customers.

2.2 Cybersecurity certification, standardisation and supply chains

Website: www.ecs-org.eu
Contributor: Roberto Cascella[13]
Senior Policy Manager

ECSO is a pan European, multi-stakeholders and cross-sectoral partnership organisation working on cybersecurity with a holistic approach, establishing and strengthening its collaboration with various other actors and stakeholders' part of the European cybersecurity ecosystem.

ECSO maintains close collaboration with European Commissioners and top-level management of the European Commission's DGs including DG CNECT, DG RTD, Members of the European Parliament (MEPs), Committees and Political Groups providing independent assessments on European legislative proposals such as the implementation of the NIS Directive, the Cybersecurity Act including the establishment of a European Certification Framework and the definition of ENISA's new mandate, as well as the set-up of a European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

During the presentation, ECSO focused on the ECSO Working Group (WG) 1 activity working on the "standardization, certification, and supply chain management". Here are some of the aspects that ECSO is trying to address:

- **Connected components**
  Work on the inter-relationship ("composition") of EU scheme certified components based on standards for trusted supply chain and product certification in line with the EU Cyber Act.

- **Digital services and systems**
  Understand the systems' and services' dependencies: needs and current approaches for risk management and operational aspects.

ECSO has contributed to the recommendation for the certification scheme of the industrial, automated control system report done with the pilot projects.

The ECSO product certification composition, known by the common criteria community and they

[13] https://cyberwatching.eu/roberto-cascella

already using it, was presented, and explain how to move it from common criteria and bring this concept in any certification scheme by:

- Enabling efficient re-use of certificate and evaluation evidence.
- Decreasing certification cost and improve overall process speed.
- Providing benefit to horizontal components specialised in application domains.
- Contributing to the time to market of certified products.

Recommendations from ECSO

It is important to look at the European cybersecurity certification and understand what could be the main challenges that could hinder the usage of future European cybersecurity schemes across industries, consideration such as:

- Cybersecurity framework consistency.
- Composition of evidence and considerations for system integrators.
- Analysis of priorities for cybersecurity certification based on market needs.

2.3 The SME guide for the implementation of ISO/IEC 27001

Website: www.digitalsme.eu
Contributor: Fabio Guasconi[14]
Chairman of DSME's cyber and data working group, and President and Founding partner of Bl4ckSwan S.r.l.

Digital SME Alliance is the largest network of small and medium-sized ICT enterprises in Europe, representing about 20,000 digital SMEs, which is a joint effort of 30 national and regional SME associations from EU member states and neighbouring countries. Digital SME Alliance is also a founding member of the Small Business Standards (SBS). SBS is one of the Annex III organisations of Regulation (EU) 1025/2012, which represents and defends SMEs' interests in the standardisation process at European and international levels.

As part of its SBS activities, Digital SME Alliance leads the SBS sectoral approach on ICT and involved in the creation of the "SME Guide for the Implementation of ISO/IEC 27001"[15], dedicated to SMEs for the implementation of ISO/IEC 27001 on information security management. ISO/IEC 27001 is the international standard for companies that need a robust approach to managing information security and building resilience. With its Guide, DIGITAL SME aims to help SMEs better understand ISO/IEC 27001 and assist them in its concrete implementation.

[14] https://cyberwatching.eu/fabio-guasconi
[15] http://www.sbs-sme.eu/publication/sme-guide-implementation-iso-iec-27001-information-security-management

How can the guide be helpful for Small and medium-sized enterprises?

1. SMEs make up the vast majority of businesses in Europe, outnumbering large corporations and employing more people. They are recognised to be a driver for innovation in Europe.
2. Most SMEs underestimate their risk level for cyber-attacks, in the belief that they do not handle any information worth stealing.
3. However, small businesses have a lot of digital assets compared to individual user and they often have fewer security measures in place than larger organisations.

The SME Guide for the implementation of ISO/IEC 27001 was developed by information security experts appointed by recognised SME and cyber-security trade associations of various European countries. The guide is written for and applicable for SMEs that rely on technological assets. Its guidelines can be easily implemented by any organisation, whatever their size or complexity.

Recommendations from DSME

The SME Guide describes a series of practical activities that can significantly help with establishing or raising information security levels within an SME. This will strengthen their business and facilitate partnership opportunities within local and EU markets.

The main advantages for SMEs using the guide are:

- Disseminating high-level information concerning information security management in small businesses,
- Increasing uptake of information security management concepts based on ISO/IEC 27001 by European SMEs,
- Having a reference document that will represent the port of call for SMEs willing sort out the wild ecosystem of information security management.

3 Solutions and resources for cyber-risk management

3.1 The Cyberwatching.eu Risk Temperature Tool

Website: www.aon.it
Contributor: Paolo Modica[16]
Research & Development Project Manager

The new **Cyber risk temperature tool**[17] produced by the cyberwatching.eu project provides a preliminary assessment of the exposure to cyber risk for SMEs. By completing this online questionnaire, any SME, business or even public administration can receive an initial evaluation of

[16] https://cyberwatching.eu/paolo-modica
[17] https://cyberwatching.eu/cyberwatching-cyber-risk-temperature-tool

their current risk to a cyber-attack and recommendations on how to reduce risk.

The questionnaire is divided into two main parts. Firstly, the interviewee is asked to give a personal assessment of his company's IT security. Then the interviewee is asked more technical questions. By assigning a score to each answer and analysing this score, a profile is assigned to the interviewee.

Recommendations from Cyberwatching.eu and AON

It is important to get a vulnerability assessment as most thorough as possible, since dangers and gaps may come from multiple sources such as i) methodologies ii) knowledge iii) distribution of administrative rights iv) information segmentation policy v) authentication policies vi) etc.

The risk management tool serves as a first entry-level to inform the user of initial steps to take. A more in-depth and complete analysis is highly recommended in order to receive a precise and tailored vulnerability assessment for one's company, though the Cyber risk Temperature tool represents a smart and rather quick starting point for both the user and the organisation.

3.2 CyberSure: Cyber Security Insurance – A Framework for Liability Based Trust

Website: www.cybersure.eu
Duration: January 2017 – December 2020
Contributor: Panos Chatziadam[18], Network Security Specialist at FORTH-ICS

CyberSure is a programme of collaboration and exchanges between researchers aimed at developing a framework for creating and managing cyber insurance for cyber systems. The purpose of creating such policies will be to enhance the trustworthiness of cyber systems and provide a sound basis for liability in cases of security and privacy breaches. The framework will be supported by a platform of tools enabling an integrated risk cyber system security risk analysis, certification and cyber insurance, based on the analysis of objective evidence during the operation of such systems.

CyberSure will develop its cyber insurance platform at TRL-7 by building upon and integrating state of the art tools, methods and techniques. These will include: (1) the state-of-the-art continuous certification infrastructure (tools) for cloud services developed by the EU project CUMULUS; (2) the risk management tool of NIS enhanced by the NESSOS risk management methodology; and (3) insurance management tools of HELLAS.

The impact of the project firstly improves the process of cyber insurance such

- Baseline risk analysis: Risk assessment methodologies and tools will support the early analysis and specification of risk models

[18] https://cyberwatching.eu/panos-chatziadam

- Certification: Generation of executable cyber system certification models and use them to carry out assessments of the soundness and the effectiveness of the countermeasures used for mitigating risks
- Comprehensive risk assessment: The certificates and/or the operational evidence generated by certification should provide inputs to a subsequent comprehensive assessment of risk that may be required for formulating and pricing cyber insurance policies
- Cyber insurance policy management: This phase covers the activities of managing cyber insurance policies, i.e., policy creation, pricing and updating and claim handling.

It also improves risk assessment for (1) cyber insurance by providing practical risk assessment targeted at organisations, who are providing cyber insurance, which leads to the enrichment of the cyber insurance sector via the application of risk assessment methodologies and innovative techniques applied for cyber services, (2) dynamic and automated risk assessment evidence collection as opposed to manual testimony-based risk assessment (remove the human factor), improving the insurance setup process and policy identification through objectives and measurable assessment of the degree of reliability, and (3) dynamic semi-automated adaptation of the insurance policy based on the evidence collected.

Recommendations from R&I project: CyberSure

The CyberSure project considered the different business impact that cyber insurers and cyber system providers in terms of delivering security services to their customer.

Cyber insurers:

- Provision of a comprehensive approach and platform for creating, monitoring and adapting cyber insurance policies, **providing cyber insurance policies customised to the needs of individual customers and their organisational risk assessment**.
- Dynamic and continuous risk management will lead to a more thorough and accurate basis for monitoring cyber insurance policies, **reducing the risk and cyber insurance management costs and consequently policy premiums.**

Cyber system providers:

- **Improving security** through the provision of automated risk management and S&P assessment and certification services,
- **Incentivising service providers** to improve their security according to reference security standards and benchmarks, to reduce their insurance premiums, and
- **Establishing liability** through the undertaking of cyber insurance policies.

3.3 SECONDO: A Security ECONomics service platform for smart security investments and cyber insurance pricing in the beyond 2020 netwOrking era

Website: www.secondo-h2020.eu
Duration: January 2019 – December 2022
Contributor: Aristeidis Farao [19]
PhD candidate at University of Piraeus

First and foremost, most of the organizations working with the internet and network services get experienced an increase in cybercrime. We need to protect our systems against the increased cyberattacks. Regarding cyber threat intelligence (CTI), we separate the CTI operations into four different phases. First, we need to Acquire Data. The data come from internal sources and external sources. Data from internal sources are related to how the organization works, the internal procedures that get used as well as the services that get used. While, the data from external sources come from social media, open-source intelligence, human intelligence, and the dark web.

Secondly, we have to Analyse the data we acquired from the first phase. For that purpose, we have many tools, like artificial intelligence, to make predictions, to extract insights and patterns. We also use data analytics to analyse raw data to make conclusions. Also, since we miss some data, we use machine learning to predict these missing values. Thirdly, we have to take action (Intelligence). Based on the previous analysis, we have to detect the threats of our organizations and evaluate the status of our organization. Also, we have to respond and prepare the organization's future actions aiming to mitigate the risks, and since we cannot mitigate them at all, we can also transfer the risk. The last phase is related to Continuous Risk Monitoring. During that phase, we continuously assess the risk level and the performance of the implemented security controls. However, we can observe that the CTI comes with many challenges, e.g., proper team, budget allocation, access to all intrusion points, understanding and integrating CTI).

The SECONDO Project proposes an Economics-of-Security-as-a-Service platform that encompasses a comprehensive cost-driven methodology for a) estimating cyber risks based on a quantitative approach; b) recommending optimal investments in cybersecurity for efficient risk management and c) determining the residual risks and estimating the cyber insurance premiums.

The SECONDO platform consists of four modules. The Quantitative Risk Analysis Module is responsible to quantitatively estimate the cyber risk exposure, utilizing data that not only come from the internal sources that are related to the valuation of the assets and the assessment of the user's behaviour, but also from external sources, using crawlers to find data in social media but also in the dark web. The second module is the Cyber Security Investment Module. This module consists of two parts, the Econometrics Module and the Game-Theoretic Module (GTM). The ECM will provide estimates of all kinds of costs of potential attacks as well as the costs of each possible security control. On the other hand, the GTM will model all possible attacking scenarios and defensive strategies and then uses game-theoretic techniques to derive optimal defending

[19] https://cyberwatching.eu/aristeidis-farao

strategies in the form of Nash Equilibria. The third module is called Cyber Insurance Coverage and Premium Module (CICPM), which is responsible not only to generate the premium but also to store it in a smart contract. The last module is the Continuous Risk Monitoring Module (CRMM) that is responsible to continuously assess the risk level and the performance of the implemented security controls. We can observe that the main modules follow the four phases of the CTI.

The impact of organizations can get reflected in four stages. The first one is related to Mitigate Cyber Risk. It can get achieved since we collect data from phishing campaigns on the organization assessing the user behaviour, we analyse data from SIEM, we collect data from social media and dark web but also, we have our asset valuation function. Secondly, the organizations can get consulted on cybersecurity strategies and investments due to the ECM and GTM. Also, we can ensure fair premiums due to the CICPM.

Recommendations from R&I project: SECONDO

- **Improve the Continuous Risk Monitoring**: More specific, a successful continuous risk monitoring will be responsible to assess continuously the risk levels, including the performance of the implemented cybersecurity controls.
- **Risk Transfer**: If the organization installed tools and methods to mitigate the risk but not in an acceptable level the risk transfer is a solution.
- **Comply with Guidelines and Regulations**: The compliance of an organization with guidelines and regulations related to cybersecurity can reinforce the organization against potential cybersecurity incidents.

3.4 The Geiger Cybersecurity Counter

GEIGER

Website: www.project.cyber-geiger.eu
Duration: June 2020 – November 2022
Contributor: Max Van Haastrecht [20]
PhD Candidate in Cybersecurity at Utrecht University

The Horizon 2020 project GEIGER aims to help micro-and small-sized enterprises (MSEs) in becoming more aware of the cybersecurity risks they face. The GEIGER application will also help users and their companies to become more resilient to cyber threats.

Using a well-known formula for risk:

Risk = Threat x Vulnerability x Consequence,

we argue that there is a discrepancy between the cybersecurity risk people feel, and the cybersecurity

[20] https://cyberwatching.eu/max-van-haastrecht

risk experts estimate exist. Generally, people underestimate risk, meaning they are less likely to feel the need to use cybersecurity risk management solutions than cybersecurity experts may think.

Part of this discrepancy comes from an inaccurate definition of 'threat' that is often used in research and other projects. To define the threat level, proxies such as the prevalence of vulnerabilities in an MSE are often used. In GEIGER, we aim to take threats at their face value. To get an accurate understanding of the frequency with which MSEs face digital security threats (e.g., phishing), we work together with Computer Emergency Response Teams (CERTs) and National Cyber Security Centres (NCSCs) throughout Europe.

The GEIGER indicator, together with the education ecosystem that the project will also develop, contributes to creating an attractive cybersecurity solution for small businesses and entrepreneurs. One of our ambitious goals is that by the end of the project, 50,000 MSEs have tried the GEIGER solution.

Recommendations from R&I project: GEIGER

Cybersecurity risk management can be handled better by MSEs:

- Researchers must commit to more accurately reflecting the concept of 'threat' in their risk management solutions. This is an important step in limiting the discrepancy in understanding of risk between theory and practice.
- Working together with CERTs, NCSCs, and other governmental organisations in cybersecurity projects is essential. Not only do they have information that accurately reflects the state of the world, but including them in projects helps to harbour trust among potential users of the cybersecurity risk management solutions we offer.
- Cybersecurity risk management is a process, not a 'quick check'. Cybersecurity risk management solutions should always aim to help users over an extended period of time, for example by incorporating an education framework.

3.5 RESISTO: RESIlience enhancement and risk control platform for communication infraSTructure Operators

Website: www.resistoproject.eu
Duration: May 2018 – October 2021
Contributor: Mirjam Fehling-Kaschek [21]
RESISTO Project Coordinator

RESISTO is an EU H2020 project with the aim of improving the risk and resilience of telecommunication infrastructures and improves their ability to handle cyber, cyber and combined cyber-physical threats. RESISTO comprises two main control loops: the long term and short term.

[21] https://cyberwatching.eu/mirjam-fehling-kaschek

The long-term control loop includes offline analysis and a risk and resilience management process. This management process extended the risk management ISO-31000 standard to include resilience assessment. Alternatively, the short-term control loop is an online process that works to detect anomalies in the system and evaluate the impact of those anomalies or adverse events. The short-term loop also provides decision support. The two control loops are connected via the Knowledge Base where indicators from both loops are compared and feedback can be given to the long-term control loop for adjustments in the simulations.

Recommendations from R&I project: RESISTO

- Resilience should be incorporated with risk management. Including resilience will allow for the systems to able to handle more adverse events, including ones that are unknown or have too low of an occurrence probability to be considered in traditional risk management.
- One of the outputs of the risk and resilience management process should be the quantitative measurement of many specific resilience indicators, each one related to a specific threat. For reasons of convenience and to reduce complexity, it is necessary to prioritize threats in terms of probability and level of impact, and then focus on the most relevant.
- When investigating threats and adverse events to improve cybersecurity, cyber-attacks should be considered, but also physical-cyber-attacks. This is to say that physical events, whether intentional, accidental or natural, may lead to problems in the cybersphere and therefore should be investigated and included in any risk analysis related to cybersecurity.
- Furthermore, in the event of physical and cyber threats that can occur at the “same” time and/or in the “same” place, even in a completely independent way, the aggregate impact should be assessed and the countermeasures to be implemented should be unified.

4 Risk management in the health sector

4.1 CUREX: seCUre and pRivate hEalth data eXchange

Website: www.curex-project.eu
Duration: December 2018 – November 2021
Contributor: Eleni Veroni[22]
Research Associate at Systems Security Laboratory, University of Piraeus

The greatest challenge for the e-health ecosystem is to find the balance among security requirements, new regulations and human welfare. Every day, more and more paper-based health records are being replaced with electronic ones, raising new risks, vulnerabilities and threats. At the same time, modern healthcare services, to function properly, require constant data sharing between stakeholders and service providers. These interconnections form a complex ecosystem

[22] https://cyberwatching.eu/eleni-veroni

with many interrelated entities, creating a very large attack surface. To secure such an evolving and complex environment from unknown vulnerabilities and new cyber threats, secure-by-design devices and services are required, as well as a risk-based approach to help the higher management to stay ahead of a potential cyber crisis.

It has been identified that the newly introduced threats against the healthcare domain are mainly targeting standard procedures applied to Electronic Health Records. One such standard procedure is the health data exchange. Health data exchange takes place intending to advance the services provided to patients today. Health data may be exchanged within the same organisation where, for example, different clinics need to share data to effectively treat a patient. Another common scenario is the one that foresees the cross-organisation transaction of medical records, where the data need to be sent to a different institution or even a different country, for further assessment.

The future of healthcare services will be highly dependent on the massive exchange of data, which, to be realized, increased connectivity is required between platforms, devices & organizations. The interconnectivity, however, creates several security issues that need to be addressed beforehand, such as zero-day vulnerabilities and advanced threats. Every attempt against healthcare infrastructures puts at risk both patients' privacy and health and may cause severe operational disruptions and major economic losses to the healthcare organizations. On top of that, the responsible authorities, through the legislation and directives enforced in European Union member countries, have created additional obligations for organizations that operate on clinical & medical data (e.g., GDPR).

CUREX, a three-year R&I Action funded under the 2018 call for "Trusted digital solutions and Cybersecurity in Health and Care", addresses comprehensively the protection of the confidentiality and integrity of health data by producing a novel, flexible and scalable situational awareness-oriented platform. CUREX allows a healthcare provider to assess the realistic cybersecurity and privacy risks they are exposed to and which are propagated to the data that is exchanged between hospitals and care centres. For this purpose, CUREX proposes a cybersecurity and privacy risk assessment toolkit tailored for different types of healthcare organisations. The toolkit is comprised of the Cybersecurity Assessment Tool (CAT) and the Privacy Assessment Tool (PAT).

CAT assesses risks related to cybersecurity threats and vulnerabilities as modelled by the CUREX vulnerability discovery process and the threat intelligence functionality. Analysing data coming from multiple sources, it estimates the risk level of an organization in real-time, performing both quantitative and qualitative risk analysis and producing cybersecurity risk scores per organisation and asset, which are stored on the CUREX Private Blockchain. CAT has the ability to propose countermeasures to address the identified risks on the fly, which are later leveraged by the CUREX decision support tool.

PAT measures the privacy level of an organisation aiming to support compliance with the GDPR for protecting patients' privacy. Based on every business process that concerns the processing and exchange of data, PAT assesses the degree of compliance of the healthcare organisation with the GDPR by providing an indicative privacy score by looking at all assets used to process sensitive data. Finally, PAT, using its Privacy Quantification Engine, merges the cybersecurity and privacy impact to quantify an overall privacy risk level, that will also be stored on the CUREX Private Blockchain.

A significant challenge that the healthcare domain needs to overcome is its closed nature due to its

criticality, complexity and strict regulation, which disallows the threat of intelligence sharing between organizations and the community in general. Repositories containing information specifically for software and hardware used in the domain are not currently available, and care centres, especially public ones, are rarely in a position to afford proprietary cybersecurity solutions.

Recommendations from R&I project: CUREX

During the first few months of the COVID-19 crisis, the attacks against the healthcare sector reached unprecedented levels. The current healthcare infrastructures, under the extreme pressure of the pandemic, are unable to handle the digital crisis happening at the same time. CUREX's aim to enhance the security level of the domain is more relevant than ever, and for this to happen the involved stakeholders should invest in tools and procedures that will:

- **Ensure the organisation's compliance with the current European legal framework**. More specifically, healthcare organisations should take action to address the requirements posed by EU legislation and directives, such as the General Data Protection Regulation (EU) 2016/679 (GDPR), the Directive 2011/24 (EU) on patients' rights in cross-border healthcare (Patients' Rights Directive), the Regulation (EU) 2017/745 on medical devices (MDR), the Regulation (EU) 910/2014 on electronic identification and trusted services for electronic transactions in the internal market (eIDAS Regulation) which introduces the mutually recognised electronic identification of patients and healthcare providers facilitating the proper cross-border provision of healthcare services, as well as the Directive (EU) 2016/1148 on network and information security (NIS Directive), and the Regulation on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (Cybersecurity Act), both of which are expected to become mandatory in the near future.

- **Improve the cyber hygiene culture among personnel.** The definition of strategies for raising cybersecurity and data privacy awareness focusing on the specific needs of different employee groups in a healthcare organization (i.e., Admin, Medical, IT, Mgmt. /Security), can help identify and close group-specific gaps through the recommendation of tailored human-centric actions/controls.

- **Minimize the impact of possible violations of the organisation's infrastructure and data.** Medical facilities should invest in cybersecurity risk management solutions, to complement and extend their existing cybersecurity infrastructures. A risk-based approach that takes into account risks not only coming from direct cyber-attacks but also knowledge gaps and legal breaches should be adopted by the higher management to address future cyber threats holistically.

4.2 *PANACEA: Protection and priVacy of hospital and health iNfrastructures with smart Cyber sEcurity and cyber threat toolkit for dAta and people*

Website: www. panacearesearch.eu
Duration: January 2019 – December 2021
Contributor: Fabrizio De Vecchis [23]
Technical Project Manager at RHEA

DRMP protects complex hospital IT infrastructures by enabling the computation of possible attack paths on multiple layers (network, access, humans, e.g., medical staff). An innovative aspect of DRMP is the multi-dimensional attack model, reflecting the role played by human behaviours in the development of a cyber-attack. The model tries to capture how human users access ICT and medical devices, identifying human vulnerabilities that can be exploited to materialise the most common threats in healthcare organisations.

Use case scenarios include:

- Gemelli University Hospital: Laboratory of Systems and connected point of care testing (POCTs).
- Irish Health Service Executive: Hospital monitor control system and wireless connected medical devices.

The presentation highlighted multi-dimensional data acquisition and reachability computation of the monitored environment; acquisition of IT infrastructure knowledge (scans, topology of data flows, asset characteristics); acquisition of vulnerability surface knowledge (scans); acquisition of users and user access information; acquisition of business and governance models. It also showed the threat analysis, risk and response evaluation, including technical, governance, organisational and human mitigation actions, as well as the visual analytics environment, explaining how the DRMP increases cybersecurity resilience of IT infrastructure in healthcare organisations.

Recommendations from R&I project: PANACEA

- Factor in human aspects and staff security profiles in risk management, analysing behaviour like the sharing of credentials and other weak links or vulnerabilities caused by negligence or carelessness. Ensure mitigation actions include training or secure behaviour nudging.
- Consider a multi-dimensional approach to risk management, across the business, access, network and human layers with attack paths for each layer to reduce organisational risk and impacts on business processes.
- To increase cybersecurity resilience in healthcare IT infrastructures, adopt new models that

[23] https://cyberwatching.eu/fabrizio-de-vecchis

can rapidly capture and analyse multiple variables in a potential attack and proactively and continuously monitor current risks, supporting operators with increased situational awareness and guided and interactive risk analysis.

- Involve end-users in testing new tools and solutions to ensure usability, effectiveness in reducing threat surface and affordability.

5 Conclusion

Cybersecurity is a pressing issue not only for large enterprises, as well as for small businesses. The fundamental risks areas are similar no matter how big the scale is, as they still hold potentially lucrative data and information. Frequently, criminals are targeting SMEs and start-ups as they are softer target with less IT security resources, and cannot invest in the same specialist technology or training as larger corporates.

Over the decade, cybersecurity has moved from a technical specialism to a mainstream business issue. Under the general data protection regulation (GDPR), small businesses now have the same responsibility as large corporations when it comes to processing and protecting data.

The Cyberwatching.eu webinar on "**Cybersecurity risk management: How to strengthen resilience and adapt in 2021**", provided practical aspects, while at the same time shared tools and references that can give organisations, particularly SMEs, MSEs and start-ups, an edge in cybersecurity risk management.

The main recommendations from this document are detailed below:

- It is important to **look at the European cybersecurity certification and understand what could be the main challenges that could hinder the usage of future European cybersecurity schemes** across industries.
- Certification can be a long, complex and expensive road for SMEs. **Providing an accessible first step to understanding the areas in which they have gaps in security** and the types of actions that they should take towards an eventual certification.
- Providing practical activities that can significantly help with **establishing or raising information security levels within an SME**. This will strengthen their business and facilitate partnership opportunities within local and EU markets.
- Dynamic and continuous risk management will lead to a more thorough and accurate basis for monitoring cyber insurance policies, **reducing the risk and cyber insurance management costs and consequently policy premiums.**
- Cybersecurity risk management is a process, not a 'quick check'. **Cybersecurity risk management solutions should always aim to help users over an extended period of time**, for example by incorporating an education framework.
- **Resilience should be incorporated with risk management**. Including resilience will allow for the systems to able to handle more adverse events, including ones that are unknown or have

too low of an occurrence probability to be considered in traditional risk management.

- One of the outputs of the risk and resilience management process **should be the quantitative measurement of many specific resilience indicators, each one related to a specific threat**. For reasons of convenience and to reduce complexity, it is necessary to prioritize threats in terms of probability and level of impact, and then focus on the most relevant.

From a healthcare perspective, the current healthcare infrastructures, under the extreme pressure of the pandemic, are unable to handle the digital crisis happening at the same time.

- **Improve the cyber hygiene culture among personnel**. Ensure the organisation's compliance with the current European legal framework which include the GDPR.
- **Factor in human aspects and staff security profiles in risk management, analysing behaviour** like the sharing of credentials and other weak links or vulnerabilities caused by negligence or carelessness. Ensure mitigation actions include training or secure behaviour nudging.
- **Consider a multi-dimensional approach to risk management**, across the business, access, network and human layers with attack paths for each layer to reduce organisational risk and impacts on business processes.

6 Contributing projects and entities

The projects contributing to this document are the following:

Website: www.cybersure.eu
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/1789/cybersure
Grant Agreement: 734815
Duration: 1 January 2017 – 31 December 2020
Contributor: Panos Chatziadam[24], Network Security Specialist at FORTH-ICS

Website: www.curex-project.eu/
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/1814/curex
Grant Agreement: 826404
Duration: 1 December 2018 – 30 November 2021
Contributor: Eleni Veroni[25], Research Associate at Systems Security Laboratory, University of Piraeus

Website: www.project.cyber-geiger.eu/
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/2126/geiger
Grant Agreement: 883588
Duration: 1 June 2020 – 30 November 2022
Contributor: Max Van Haastrecht[26], PhD Candidate in Cybersecurity at Utrecht University

Website: www.panacearesearch.eu
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/1270/panacea
Grant Agreement: 826293
Duration: 1 January 2019 – 31 December 2021
Contributor: Fabrizio De Vecchis[27], Technical Project Manager at RHEA Group

Website: www.resistoproject.eu
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/1974/resisto
Grant Agreement: 786409

[24] https://cyberwatching.eu/panos-chatziadam
[25] https://cyberwatching.eu/eleni-veroni
[26] https://cyberwatching.eu/max-van-haastrecht
[27] https://cyberwatching.eu/fabrizio-de-vecchis

Duration: 1 May 2018 – 31 October 2021
Contributor: Mirjam Fehling-Kaschek[28], RESISTO Project coordinator

Website: www.secondo-h2020.eu
Cyberwatching.eu mini-site:
www.cyberwatching.eu/projects/1972/secondo
Grant Agreement: 823997
Duration: 1 January 2019 – 31 December 2022
Contributors: Aristeidis Farao[29]
PhD candidate at University of Piraeus

Here are participating experts from SME clusters and companies:

Website: www.ecs-org.eu
Contributor: Roberto Cascella[30]
Senior Policy Manager

Website: https://www.sgsgroup.it/
Contributor: Lucio Gonzales-Jimenez[31]
CyberLab Madrid Manager

Website: https://www.digitalsme.eu/
Contributor: Fabio Guasconi[32]
President and Founding partner

Website: http://www.aon.it/
Contributor: Paolo Modica[33]
Research & Development Project Manager

[28] https://cyberwatching.eu/mirjam-fehling-kaschek
[29] https://cyberwatching.eu/aristeidis-farao
[30] https://cyberwatching.eu/roberto-cascella
[31] https://cyberwatching.eu/lucio gonzález-jiménez
[32] https://cyberwatching.eu/fabio-guasconi
[33] https://cyberwatching.eu/paolo-modica

Watch the recorded workshop video now!

You may also download the speakers' presentations on the webinar page.

How to reach us

cyberwatching.eu
The European watch on cybersecurity & privacy

www.cyberwatching.eu

@cyberwatchingeu

in/company/cyberwatchingeu

cyberwatching.eu consortium

Trust-IT Services
Communicating ICT to markets

Oxford e-Research Centre

UNIVERSITY OF OXFORD

ICT LEGAL CONSULTING Balboni Bolognini & Partners

European Digital SME Alliance

CONCEPTIVITY

360 SECURITY

AON

aeiciberseguridad
Agrupación Empresarial Innovadora CIBERSEGURIDAD y Tecnologías Avanzadas

cyberwatching.eu has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740129.