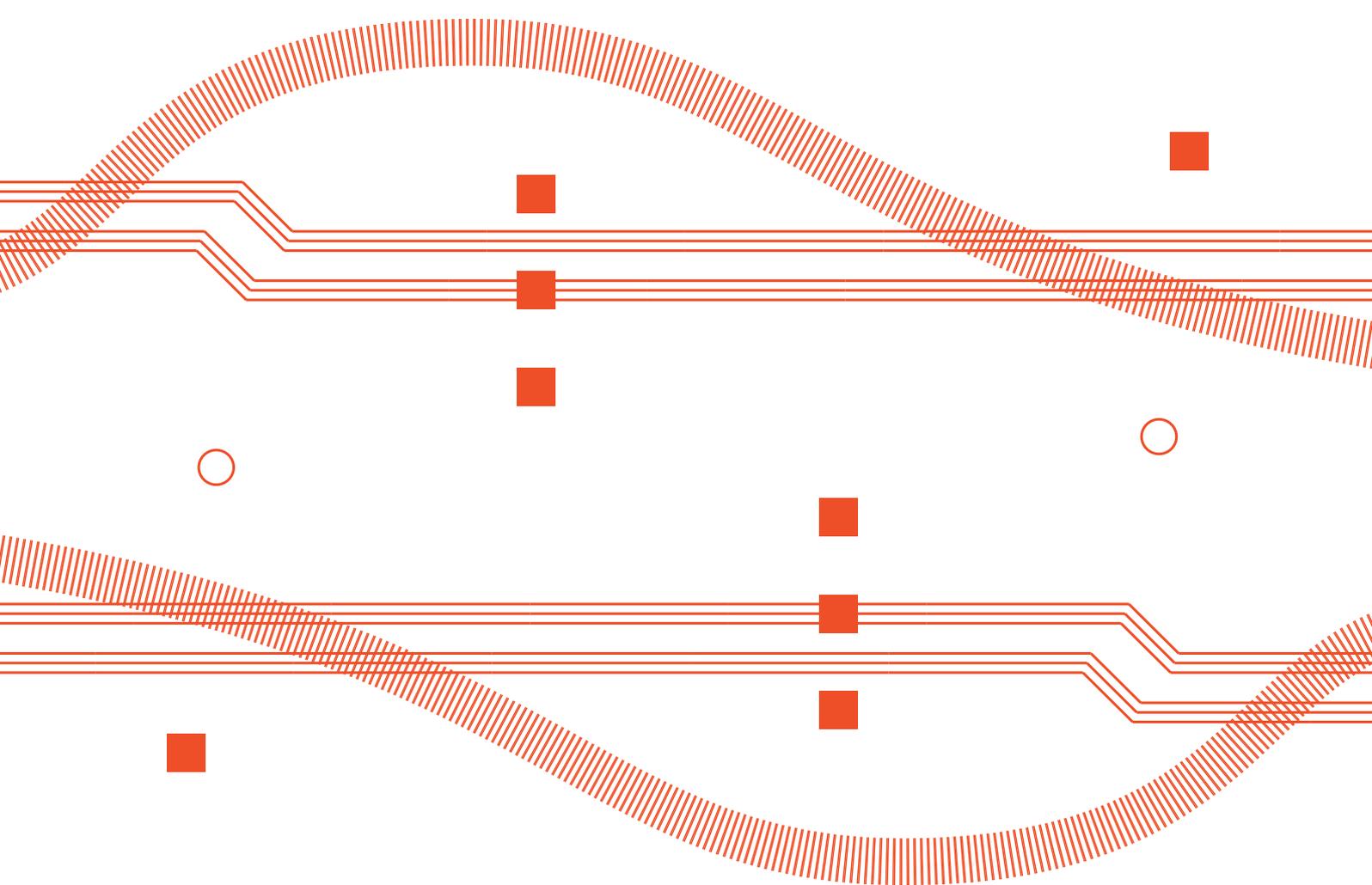


CONCORDIA
Cyber security cOmpeteNCe fOr Research and INNOvAtion

Risk Assessment and Planning
Understanding risks and their associated costs are key for a better

Roadmap for **Economics**



6 Roadmap for Economics

The economic dimension of cybersecurity has attracted only recent attention, although, a few steps had been performed under the umbrella of selected research projects on the national and international level during the past decade. Nevertheless, for research purposes, the design of new security algorithms, the development of quantum security, and the embedding of these and existing ones into prototypical and later vendor-specific solutions had been a major focus. Highly specialized companies develop single and multi-step technologies to counterattack a variety of security threats, as the overview of CONCORDIA's D4.1 shows. However, away from the more general approach is required to (a) understand, (b) design, (c) evaluate, and (d) apply security means for a given IT system, embedded in a larger organization and its processes. Thus, the scope of CONCORDIA's T4.3 is especially the economic dimension of cybersecurity perspectives, which do help to determine a very useful, applicable, and concrete Cybersecurity Roadmap for Europe.

There exist only a few complementary approaches and perspectives looking at the economics of cybersecurity. Most approaches to analyse are targeting cost-benefit trade-offs faced by users, their strategic, tactical, and operational choices, and outcomes in terms of impacts for participants, which basically resembles risk assessment – frequently used for these analyses – and needs to embed this into a strong phase-based model to become applicable.

6.1 Landscape of Economics in Cybersecurity

Often systems fail because the organizations do not bear to assess the full costs of a failure neither the risks involved. This problem is prevalent in companies and end-users that present budget restrictions to invest in cybersecurity and technical expertise, such as Small- and Medium-sized Enterprises (SME) and start-ups [67]. Therefore, investments in cybersecurity solutions (e.g., based on software, services, or hardware) that not just offer protection against cyberattacks but also help during the planning and decision process of Cybersecurity is critical for the next years, which can contribute to a reduction of both CAPEX and OPEX while offering efficient protections for businesses with different demands.



Figure 9: Key factors effecting cybersecurity economics

Figure 9 depicts the set of key factors that have to be considered when considering the economic impacts of cybersecurity in business. The lack of investments by SMEs in cybersecurity, for example, is a concern for the next years. In general, these companies have restrictions and small budgets to invest in cybersecurity. Besides the fact that large companies have been investing several amounts in maintaining a dedicated cybersecurity team, the reality of SMEs is the opposite. Frequently SMEs assigned the task of protecting their systems to IT personnel who do not have adequate technical expertise in cybersecurity. Also, since they are also involved with various IT tasks, it leads to a negligence of an assessment and management of different dimensions of cybersecurity that impact the business. Concerning risk analysis and their associated economic impacts, investment in education, and training activities are extremely necessary from a cybersecurity viewpoint. Therefore, it is possible to train decision-makers to analyse their systems through a holistic view, correlating the economic impacts of security activities (e.g., education, measures of prevention and remediation, insurance) with its economic impact to prevent losses from cyber insecurity. Furthermore, a well- defined and continuous education program can be considered to strengthen the capacity of the employees to identify and report frequent attacks (e.g., social engineering and phishing). Furthermore, education

can help to build a robust Cybersecurity knowledge in the business, where can reflect on the capacity of the business to handle more complex situations such as ransomware or a botnet attack scenario.

The proactive planning for cybersecurity is also a crucial step toward a well-defined and efficient cybersecurity strategy. Thus, proactive planning should focus not only avoid attacks that can surpass the business infrastructure but also on how to mitigate or recovery from a cyberattack, such as acquiring protection services or even contracting a cyber-insurance for specific scenarios. However, before the proactive planning, it is important to conduct an in-depth risk assessment, which can identify the different vulnerabilities, attack vectors, and economic impacts of the different systems and sub-systems that compose the business. It is a critical task since a wrong assessment might result in a cascade effect, such as investments in cybersecurity and planning that do not covers the critical elements of the business.

6.2 Applied Economics Cornerstones

Cornerstones are considered to be architecturally necessary, especially to avoid the falling apart of the building. Thus, the following three dimensions determine for CONCORDIA's T4.3 these stones, which relate essential economic investigations with major security mechanisms and dedicated areas of application. Besides those three dimensions as key ones as of today, other directions might be relevant to be investigated, such as fully decentralized system architectures, Service Level Agreement (SLA) enforcement, and remote electronic voting.

6.2.1 Determination of Cyber Crime Costs

Determining the costs of cybercrime is a key factor for understanding Cybersecurity from an economic perspective. However, such a determination cannot be considered to be a straightforward task, since different cost categories and elements have to be considered during this process. Examples of these costs include:

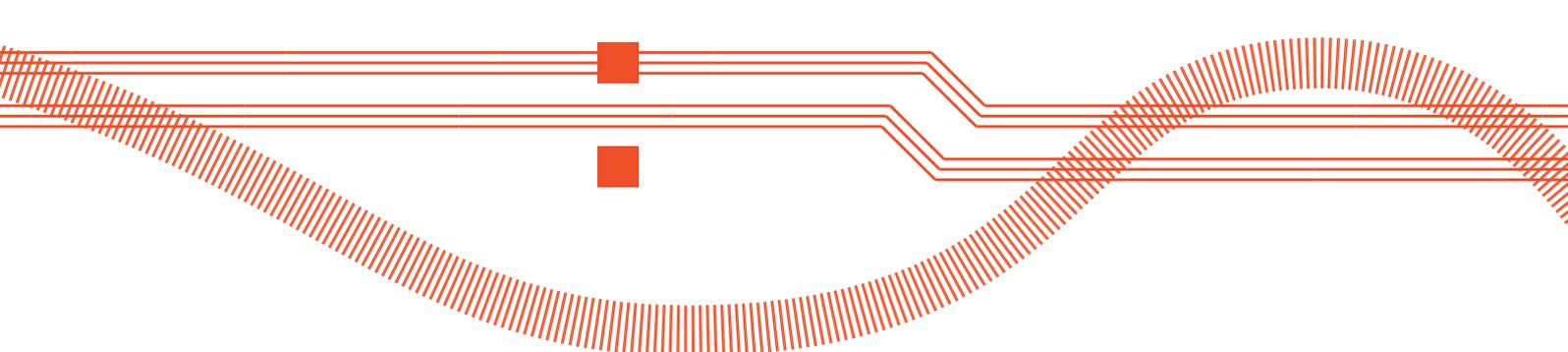
- **Cost of anticipation:** includes preventive security means, such as access control or firewalls
- **Cost of direct consequences:** includes an interruption of service due to Denial-of-Service attacks or a reduction of availability due to unreliable communication services

- **Cost of reactive security:** typically covers restoring backups, paying fees for a certain non-compliant component, or cybersecurity insurance premiums.
- **Cost of indirect consequences:** includes reputational damage, loss of confidence, or closures of the business.

A second relevant aspect is the benefit analysis in terms of a Return-On-Security- Investment (ROSI). This analysis includes links between security assurance levels and macro-economic impacts. Thirdly, the perspective to investigate societal costs, externalities, and network effects become relevant but make cybersecurity economics different. Since some economic studies of cybersecurity in the framework of demand/supply models (i.e., a cybersecurity market) exist, the decomposition into different segments (e.g., hardware, software, or services) as well as different operations and phases, become possible. Finally, further studies focus on incentives, behavioural economics (such as in the case of privacy), the economics of adversaries (attackers), cyber-insurance models, or economic effects of cybersecurity information sharing.

6.2.2 Security Analysis and Risk Analysis

One of the fundamental aspects of cybersecurity is the knowledge about the potential risk to which systems are exposed, such that a malfunctioning or a denial of services may be observed. It is important not only to determine how to analyse risks but also to determine which of these systems under analysis are critical and require adequate measures to guarantee their security at acceptable levels. Furthermore, from a generic perspective, security cannot be analysed in a fully deterministic manner, but only under certain assumptions probabilistically, i.e., there exists no perfectly secured system, which can finally resolute as secure (or even 'safe' concerning humans involved), but for an acceptable percentage of risks, thus, for a set of an acceptable level of vulnerability the willingness to accept such a system's operation, the system can be considered operational. Another factor that contributes to the increase in complexity of today's IT systems risk analysis arises from the fact that critical systems are often interconnected with other systems and faults or vulnerabilities in any of these may lead to the strong exposure of correlated others. In this context, it is imperative (a) to understand all and especially significant dependencies between complex and distributed system components (e.g., for supply-chains or eGovernment management systems) and (b) to determine, specify, and prioritize security and safety risks associated with each actor of relevance in the use case under investigation.



The essential premise to accept or refuse a certain percentage of risk invariably requires the uniform use of risk analysis approaches across multiple systems, which are based on the measurable outcome of a system's security analysis under well-defined circumstances. Systems often are vulnerable, because organizations do not consider the complexity involved in providing a certain level of security for a large or even distributed system (i.e., correlated with other systems and subsystems as well as components). Associated costs often include two critical categories ^[68]:

- **Security (prevention of malicious activities):** investments are typically complex, because malicious activities typically expose externalities as a result of under-investment in cybersecurity, i.e., they usually exploit vulnerabilities unforeseen during the design space.
- **Safety (prevention of accidents or faults):** originates from requirements, which take systems failures due to unexpected events (i.e., natural disaster and/or human failures) into account to prevent the loss of lives.

A holistic and systematic view of complex systems is required to identify and isolate interfaces with directly connected systems for their assessment of risks and vulnerabilities in terms of safety and security. Besides, while the risk assessment seeks to determine exposure to vulnerabilities, the security analysis seeks to associate prevention and remediation measures in several categories, depending on the type of system in question.

For example, AFCEA (a non-profit organization serving military, government, industry, and academia) presented a discussion on cybersecurity economics in a practical framework ^[69]. The framework guides private organizations and the U.S. government highlighting principles to guide investments mapping risks their associated economic impacts. Threats are categorized according to their complexity i.e., sophisticated or not, and their mission criticality i.e., define how specific vulnerability could impair a service/process.

Concerning the mapping of risks and threats, the National Institute for Standards and Technology (NIST) developed a model for guiding the investment in Cybersecurity countermeasures. Specifically, NIST's Special Publication 800-37 ^[70] and 800-53 ^[71] define the Cybersecurity Risk Management Framework (RMF) including a method for assessing the implementation of controls to mitigate risk. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework to classify risks, as well as the AFCEA mapping of risks,

allows for the establishment of economic models based on threats. Although 800-37 and 800-53 do not present an analysis directly related to economic aspects, the NIST framework (as well as the AFCEA) to classify risks, allows for the establishment of economic models based on threats.

NIST defines risk as a function of the likelihood of a threat event happening, and the impact, the adverse effect, such an event has on the organization [70]. Thus, measures for both impact and likelihood, and the function by which to compute the resulting risk must be defined. Given the difficulty in assigning an absolute value to these measures, it was preferred to use a five-step qualitative scale as presented in Table 7.

To estimate the risk associated with an event, first, it must be defined which the impact of this event is in case that it occurs. Table 8 presents the five steps of the impact severity.

Severity	Description
Very High	The event would have multiple severe or catastrophic adverse effects, in such a way that recovery might not be possible.
High	The event would have a severe or catastrophic adverse effect, in such a way (i) to cause a severe degradation or loss in mission capability; (ii) cause major damage to assets and/or financial loss; or (iii) result in human death or injury.
Moderate	The event would have a serious adverse effect, in such a way (i) to cause degradation in mission capability but its extent and duration would still allow an organization to perform its primary functions; (ii) result in significant damage to assets and/or financial loss; or (iii) result in significant human injury
Low	The event would have a limited adverse effect, in such a way (i) to cause degradation in mission capability but its extent and duration would still allow an organization to perform its primary functions (ii) result in minor damage to assets and/or financial loss; or (iii) result in minor harm to individuals.
Very Low	The event would have negligible adverse effect.

Table 7: NIST impact definitions

Another valuable input for the analysis of risks is provided by ‘The Open Web Application Security Project’ (OWASP), which is an online community and non-profit organisation founded in 2001. The goal of OWASP is to produce freely available content on the topic of web application security. Since its inception it has become the de-facto standard in the field, with other reputable entities, for example, the NIST or PCI Security Standards Council regularly referencing OWASP’s work as an integral step to mitigating web application security risks. The OWASP Top10 focuses on identifying the top 10 most serious web application risks in broad terms, but each organisation is unique. As such, it is important to develop a risk analysis to determine accurately the level of risk of a system.

Additionally, specific guides/frameworks exist for different cyber systems and applications. Threat modelling is a process, which identifies possible threats or vulnerabilities in the system and assesses their danger. The goal of threat modelling is the prioritization of threats, so that

Table 8: NIST likelihood definitions

Frequency	Description
Very High	The threat source is highly motivated and sufficiently capable and is almost certain to initiate a threat event. The controls put in place are ineffective.
High	The threat source is highly motivated and sufficiently capable and is highly likely to initiate a threat event. The controls put in place are ineffective.
Moderate	The threat source is motivated and capable. The controls put in place might impede the adversary.
Low	The threat source lacks the motivation or is not capable of initiating a threat event. The controls put in place might severely impede the adversary.
Very Low	The threat source is neither motivated nor capable of initiating a threat event. The controls put in place are effective.

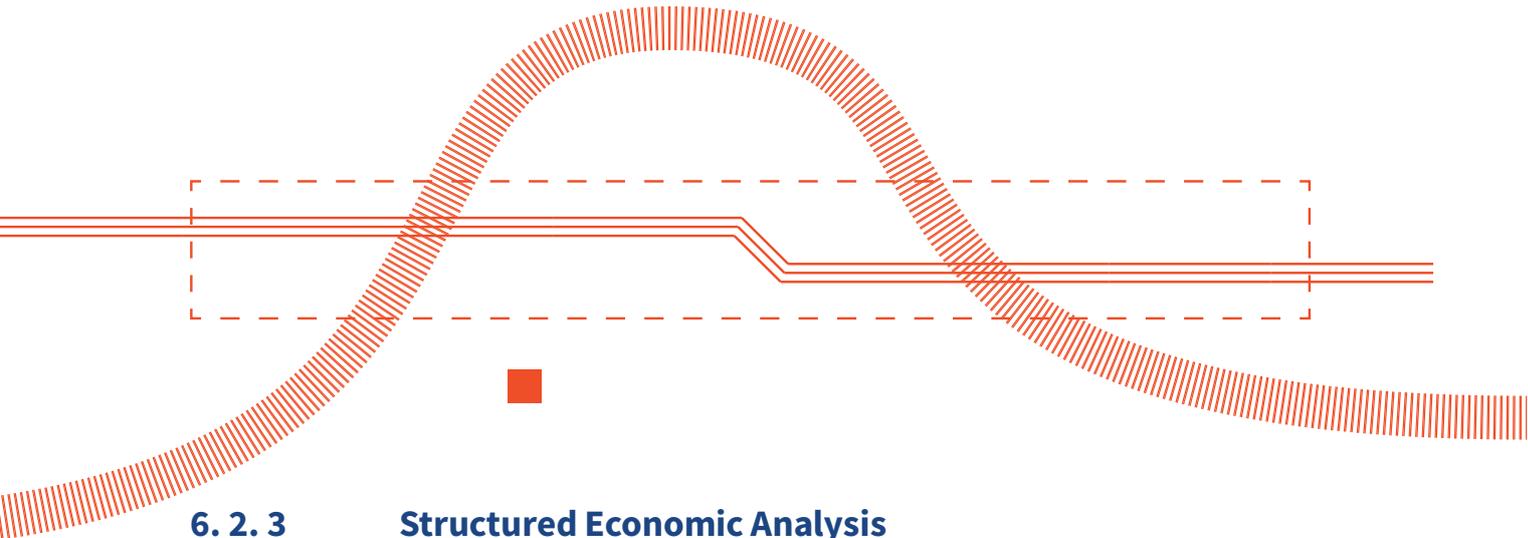
appropriate mitigation can be selected. For example, while NIST guides focus on the overall risks of an organisation, STRIDE ^[72], LINDDUN ^[73], or DREAD ^[74], map each specific type of threat as well as their mitigation actions. For instance, STRIDE (Spoofing, Tampering, Repudiation, Information (disclosure), Denial-of-Service, and Elevation of Privilege) is an industrial-level methodology that comes bundled with a catalogue of security threat tree patterns that can be readily instantiated. DREAD is a mnemonic (Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability), which, although similar, represents a different approach for assessing threats. LINDDUN builds upon STRIDE to provide a comprehensive privacy threat modelling.

Aiming at the evaluation of economic risks, ^[75] proposes a proactive model to simulate economic risks of CNI's with integrated operations, i.e., that links many vendors, suppliers into the same ecosystem. The authors seek to map inter-dependencies amongst actors to establish a causal relation, which can be used to estimate economic risk under various scenarios. However, despite providing a view on the inter-dependencies between the actors, the proposed model does not consider problems that may later occur because of a rush to attain initial economic gains.

Cybersecurity is asymmetric by nature. For example, consider an email service in which only legitimate users can access their mailboxes: even such a system can be composed of various subsystems, such as a front-end, database, access control components, and email reading and sending components. An adversary has numerous possibilities for attacking the system. Any subcomponent could be compromised independently. An attacker for example might attack the front-end, injecting code, which when executed in the context of a legitimate user's browser, leaks information, or the attacker might exploit a vulnerability in the operating system. In contrast, engineers developing and implementing security measures must consider the security of the entire system. Covering all possible attack scenarios are simply not feasible. Thus, to discuss attack surface and attack vectors, first, it is necessary to define,

which are the components to protect, and the motivation and skill level of possible attackers, to assess the probability and impact of an incident happening.

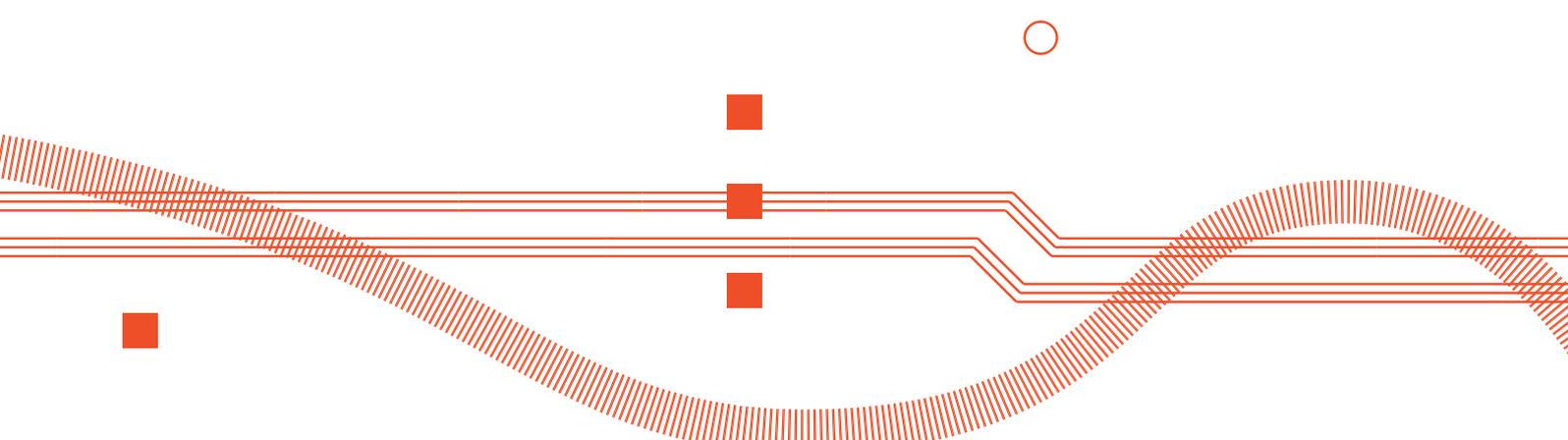
Furthermore, any rational approach in defining what is ‘appropriate’ involves (a) identification of risks by examining potential vulnerabilities and their chances of successful exploitation, (b) the cost of these results if vulnerabilities are exploited, and (c) the cost of mitigating vulnerabilities. The risk analysis is the fundamental stage toward mapping costs associated with Cybersecurity. It is responsible for determining, proactively or reactively, possible vulnerabilities/threats (i.e., likelihood as defined in Table 8) that may occur as a function of time as well as their associated countermeasures.



6. 2. 3 **Structured Economic Analysis and Recommendations**

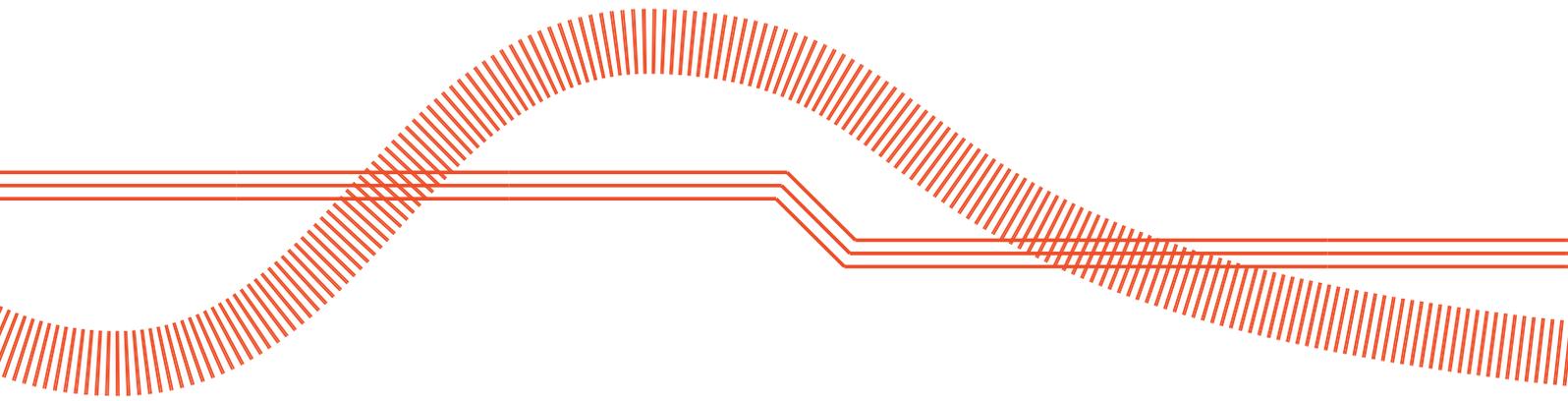
The challenge concerning a structured cybersecurity economic analysis stem from the complexity to analyse the impact of successfully exploited risks in large, distributed systems since their components are often interconnected with other systems and are exposed to different types of flaws and vulnerabilities (intentional or unintended). Thus, failures or vulnerabilities in particular components of a system may lead to the failure of the entire system or directly or indirectly correlated systems, increasing the economic impact in a non-deterministic manner. For that, a framework called SEconomy^[76] had been proposed to guide a structured risk analysis of a business, determined by a specific use case or IT system’s installation, from a strictly economic point of view, considering that often critical and important systems or components can lead to lacking relevant investments in related security activities being neglected. These include, for example, training and education of security experts, software upgrades and maintenance, monitoring activities, among other tasks. Therefore, SEconomy describes a framework to assess the efficiency of security investments in cyber ecosystems, aiming to identify economic inefficiencies concerning the risk to which a system, its components, and related systems, which are exposed in face of its security investments.

Currently, there are many on-demand protection services and marketplaces available, which are not only offering protection services but also offer technical or organizational alternatives regarding the deployment and management of such services. However, it is not a trivial task for end-users to select any of them, since many details may not be known to the user or are omitted due to falsely assumed simplifications. For that reason, MENTOR^[77], a protection recommender system, had been proposed as a supporting tool for practical guidance in cybersecurity management, being able to recommend services for the prevention and mitigation of cyberattacks. The initial steps of MENTOR investigated similarity measure techniques to correlate information, such as budget constraints and the type of service required, from customers with different services available. Based on this, MENTOR can indicate an adequate service to protect infrastructures according to different demands, such as region, deployment time, and price conditions. Although a large number of protection services are already available in the market, this number will arise together with a global deployment of novel paradigms, such as NFV and SDN. Additionally, novel business models can be used as an incentive for the development of innovative cybersecurity solutions. Based on that, a recommendation system should be able to understand the nuances of services running on different technologies to recommend a service efficiently. Besides, mechanisms to deploy the service directly on the customer's infrastructure or in a third-party host should be available, thus simplifying the process of acquisition of such protection services by non-expert end-users while reducing both Capital Expenditure (CAPEX) and Operational Expenditure (OPEX). Therefore, systems like MENTOR are important during the process of understanding and planning cost-efficient cybersecurity strategies based on the demands of a business.



6.3 Challenges

The economics of cybersecurity started more recently to become a major pillar for the operations and costs associated with cybersecurity-related investments. While the demand to provide even stronger security measures to IT system already deployed in society – starting



from the individuals' home desktop, laptop, or entertainment system, reaching over to commercial IT systems of lower to higher complexity for business and production as well as maintenance use (which include society-critical processes), and leading to administrative and governmental services (including democracy foundations such as voting), is very visible in today's society, their dedicated importance does clearly vary. Due to their very high degree of interactions, embedding, and cooperation, the different stakeholders' expertise, as well as budgets, are required to be taken into consideration upon evaluating the usefulness of an IT system as a whole or a component. Only if the demanded level of 'bulletproof' characteristics can be reached for a given situation and requirements are met and provided in full, the functional operation can be assured in a more open setting of today's IT services. Thus, the cost barriers of selected stakeholder's perceptions are key and need to be identified and measured such that individual stakeholders will have the chance to determine, at which costs the demanded level of security may be reachable before the decision on certain cybersecurity mechanisms has to be taken.

Therefore, the economics of cybersecurity will pave the path for many steps to be followed soon, especially to enable an optimization of investment, installation, maintenance, and operations, and a useful update of costs. Although CONCORDIA did start this process by determining an approach for such an analysis, a much broader team of economic experts is required in very close cooperation with security experts in different industrial and governmental domains. Such collaboration can develop a more detailed, formal, and suitable model for determining impacts of implementing technological options based on a non-trustworthy and averaged or even randomized economic cost estimation, purely driven by IT departments and typically as of today still excluding proper risk assessments. One of the main challenges for a precise economic analysis of cybersecurity includes Information Asymmetry, which makes it extremely hard to determine the different information required for a precise assessment of all cybersecurity costs. This incomplete and inaccurate information results in non-efficient cybersecurity planning and

for the investments. Therefore, main economic incentives also have to be considered to support suitable and privacy-preserving information-sharing regarding potential and experienced threats to create a strong, overarching community being able to share and predict major and minor economic and technical impacts of cyberattacks. Besides that, the mapping of different systems, processes, and their relations are crucial for the identification of all possible direct and indirect costs of a cyber- attack.

Figure 10 provides an overview of those relevant directions, which are to be covered by academia, industry, and governments as of today. This does need a mid- term and a long-term view to reach an adequate level of Cybersecurity to reduce considerably economic impacts of cyberattacks. Different challenges will arise for Cybersecurity in the next years and decades since Cybersecurity management addresses always a moving target. As technologies are evolving fast and they become part of the entirety of today’s society, such as the example with the adoption of cloud computing for many businesses and the demands on 5G as an enabler of modern mobile services, it will remain very difficult to predict impacts of cyber- attacks in the future. However, it is possible to determine (a) a clear strategy, (b) a suitable model (possibly being use case-dependent), and (c) define suitable analysis frameworks and their inherent mechanisms to prepare society and businesses, who will face new threats ahead of us.

6.4 Roadmap for Economics

Based on the current set of investigations and findings of Concordia’s T4.3, different aspects have to be considered to measure direct

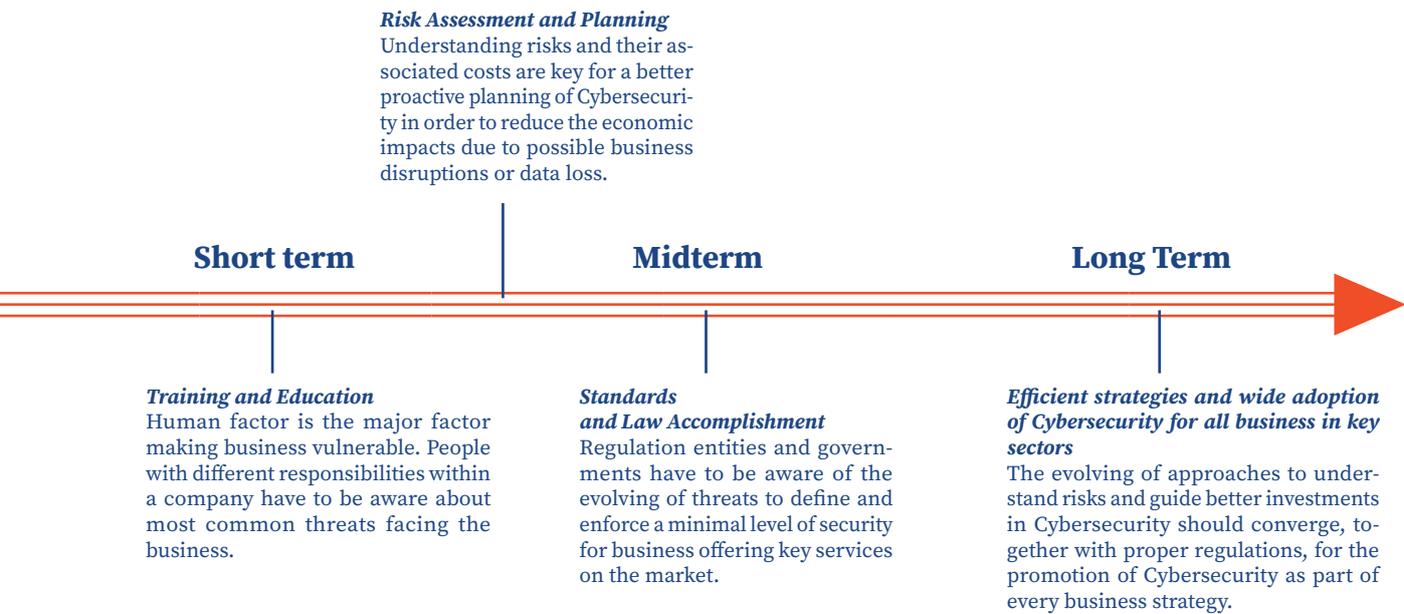


Figure 10: Overview from an Economic perspective of most important directions, steps, and threats for short-, mid-, and long-term timelines

and indirect costs of the Cybersecurity and its lack thereof. For that, an understanding of legal, economic, societal, and technological aspects is essential, since every single variable can potentially result in financial losses or a business disruption. Investments in Cyber-security are at the first glance surely not about to reach profits, but on the contrary to avoid expectable losses by knowing about threats and their countermeasures.

Thus, a set of recommendations (R) is provided below, which may see changes or adaptations in how companies think about and operate with their IT investments in general or specifically. The non-exhaustive list by T4.3 includes as of below relevant recommendations derived from current observations:

- **R1: Focus on the risk assessment and planning of cybersecurity:** An essential task for any organization wanting to gain insights into its systems' security is a risk analysis. In this task, it is essential to apply suitably (i.e., applicable for a particular system or scenario) risk analysis models to those systems in question to identify, e.g., failures and estimate probabilities of cascading failures in complex systems. Such complex systems are often characterized by the multiplicity of components or linked subsystems with which they operate in a coordinated and interconnected manner, where often failures or vulnerabilities in connected subsystems may compromise information throughout the system. In this sense, there are risk management frameworks both for mapping flaws in generic systems and specific to subsystems, which have to be observed when relevant. Once risks are assessed, the management of these risks involving possible mitigation actions involves analysing the probabilities of such risks being mitigated. In this sense, the probability estimation is based on data available locally concerning the system's security or subsystem in question (e.g., at least for credential harvesting, mapping, and scanning behaviour).
- **R2: Efficient investments on protections:** Based on the prior understanding that recommendations are observed and applied as a whole and not isolated as such, the mapping of economic impacts (i.e., investments) occurs in mapping and risk management. In this sense, the mapping of risks and their probabilities of occurrence are a fundamental input to guide economic investments and to prioritize, in an efficient way, investments related to cybersecurity of those components and subcomponents involved. For example, it is necessary to assess trade-offs between risk probabilities and the budget available to prioritize which proactive and reactive actions can be taken. The estimated probability that vulnerabilities are exploited in non-critical systems is at certain levels acceptable to the organization. However, the common logic of the more extensive the budget is, the more reactive and proactive risk mitigation

actions are possible, results in lower risk probabilities. A typical example is related to the availability of servers in data centres, to which the less likely a server is to be unavailable, the greater the cost of the service given the different actions that a provider must take to ensure that the service will remain available. It is observed, in this sense, that actions can occur in the proactive scope as preventive measures (e.g., investment in education and up-to-date courses for professionals, monitoring and updating of components), as well as reactive measures of remediation and mitigation in case of attacks (e.g., in case of responses for DDoS attacks, exploitation of vulnerabilities, or natural disasters impacting service availability).

- **R3: Standards and Law accomplishment:** When preparing a cybersecurity strategy, one of the critical factors is to map all required regulations correctly (e.g., GDPR) and standards to follow, while the technical functionality of the system has to remain as specified and the security dimensions to be tackled remain cost-efficient. If these requirements – typically a larger set of those, partially even contradicting – are not well-defined, many negative impacts can appear, such as penalties regarding data privacy violation, reputation harm, or even additional costs to mitigate cyberattacks, because of the absence of a clear standard to handle such situations. In the future, for example, companies that do not accomplish the EU Cybersecurity Act can see their image and competitiveness being impacted negatively.
- **R4: Cost reduction by using state-of-the-art technologies and approaches:** Costs involved in the implementation of cybersecurity approaches are among the main factors that impact a large adoption of cybersecurity. These costs include CAPEX and OPEX. The first one is related to the acquisition of new hardware and equipment as well as new security services to handle and deal with cybersecurity, while the second one reflects the costs of operating those cybersecurity solutions. To reduce both costs and, consequently, the total costs of the cybersecurity investments, trends of advanced and even new technical solutions have to be considered. For example, cloud-based solutions and NFV can play a key role in reducing CAPEX, while simplifying and reducing OPEX by sharing dedicated activities with third-party providers.
- **R5: Training and Education:** Most of those cyberattacks known so far are dependent on a successfully performed social engineering attack, which is amplified in case of absent or very low cybersecurity education. Investment in employees' education is the key to reduce many attack vectors (e.g., phishing, ransomware, and malware). Besides that, as soon as cybersecurity becomes complex, even better training is required, which includes besides individual users CERTs, too, to react to an imminent attack efficiently. Therefore, continued training,

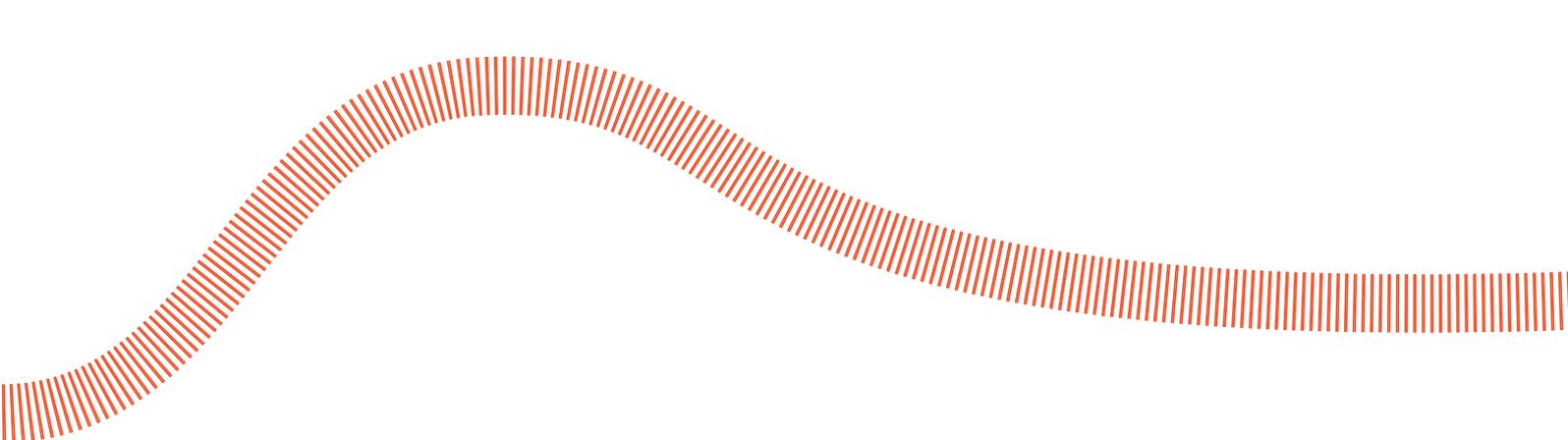
certification, and education programs (cf. Element 4 of this roadmap) are directly related to a reduced financial loss rate due to a cyberattack.

- **R6: Overall Integration of Cybersecurity Economics Modules within EU Cybersecurity:** As different architectures have been proposed for the EU cybersecurity, the overall integration of economics modules being offered as services part of a complete ecosystem may be beneficial for all stakeholders involved. This allows for thinking and enabling cybersecurity measurements in a technical dimension but also taking into account an integrated view combining different perspectives, such as economic, societal, and legal.

6.5 Taking Stock: SOTA & the CONCORDIA Leadership

Considering the cyber-economics' viewpoint, the CONCORDIA project contributes to the state-of-the-art (SOTA) in a holistic manner by providing a detailed analysis of impacts on major cybersecurity-related use cases (e.g., risk analysis and cyber insurance) based on a structured framework and prototype of solutions. This approach ensures the addressing of key economic aspects related to the future of cybersecurity, especially (i) the investigation of the cyber insurance market and the proposal of novel cyber insurance solution for risk transfer; (ii) the development of tools for risk mitigation based on state-of-the-art techniques (e.g., Machine Learning and Blockchain) focused on reducing the economic burden on business; (iii) the exploration and proposals of strategies for the recommendation of protections and economically optimum investments in cybersecurity, especially focusing on SMEs (Small and Medium-sized Enterprise); and finally (iv) the mapping of steps related to cybersecurity economics in a practical framework that can be used as a basis for mid and long-term solutions to improve cybersecurity in Europe regarding the economic impacts of cyberattacks.

Major contributions relate especially to the synergy between (a) complex tasks involving the mapping of risks with their possible associated economic impacts based on proactive or reactive mitigation measures and (b) adequate investments in cybersecurity strategies regarding, for example, security equipment, protection services, and training. Thus, a structured framework allows for detailing which risks can be assumed



6.6 Contributions for EU Policies: Economic View

Economic aspects of cybersecurity must be considered carefully to define respective EU policies since the adoption of regulations and many dimensions from an economic nature influence their effectiveness. For example, the budget available to invest in cybersecurity, the cost and knowledge required to follow regulations, and the training and certification of employees play crucial roles at different levels. The work being developed in CONCORDIA within T4.3 has direct and indirect effects onto the short, mid, and long-term adoption of cybersecurity policies and provides a valuable roadmap supporting the discussion of priorities and paths to follow.

Considering the General Data Protection Regulation (GDPR), for example, it is important to promote as many as possible security tools (e.g., analysis and monitoring solutions) that support SMEs and MNEs (Multinational Enterprise) to follow various regulatory requirements. Thus, increasing the overall security of IT systems within a company while reducing impacts on the European economy due to possible penalties applied to companies that do not follow the regulation can lead to operational and economic benefits. However, the economic concern in place relates to a broad range of companies that do not (yet) have a sufficient budget or expertise to follow such specific regulations. This can be solved potentially by achieving a more cost-efficient planning and deployment of cybersecurity measures, which will become even more challenging for the next generation of businesses and networks, such as those introduced by complex IoT (Internet-of- things) scenarios, AI- (Artificial Intelligence) based approaches, and (fully) decentralized systems.

Also, the EU Cybersecurity Act will play a critical role in the next steps of cybersecurity in Europe since, among other benefits, it establishes a cybersecurity certification framework for products and services. However, there still exist economic barriers that must be tackled to achieve fair competition in the cybersecurity market, especially for both SMEs and MNEs. Henceforth, training professionals and enhancing security tools considering up-to-date threats and vulnerabilities is a strategy that must be considered toward adopting regulations without large amounts of financial budgets. This is also directly related to culture change, where companies have to consider cybersecurity and respective mechanisms as an investment rather than an additional cost.

Please note, that this is a part of the CONCORDIA Roadmap. If you are interested in the whole document, you can download it **here**.

- [68] T. Moore. 'The Economics of Cybersecurity: Principles and Policy Options'. International Journal of Critical Infrastructure Protection, 3(3):103–117, (December 2010).
- [69] Afcea Cyber Committee. 'The Economics of Cybersecurity: A Practical Framework for Cybersecurity Investment'. International Journal of Critical Infrastructure Protection, pages 1–15, October 2013.
- [70] G. Locke and P.D. Gallagher. Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach. Technical Report NIST Special Publication 800-37 Revision 1, National Institute of Standards and Technology, Gaithersburg, MD, USA, (December 2019). Accessed Dec. 18, 2020.
- [71] Information Technology Laboratory. **Security and Privacy Controls for Federal Information Systems and Organizations**. Accessed Dec. 18, 2020.