Cost-Effective and Accessible Cybersecurity for Digital Finance SMEs

H2020 CyberKIT4SME Project White Paper

December 2022

https://cyberkit4sme.eu/

JRC Capital Management and Consultancy GmbH Berlin, Germany

Digital Finance and the importance of Cyber Security

The finance sector consists some of the most critical infrastructures that *support* our societies and the global economy. In recent years, the critical infrastructures have become more digitalized and interconnected than ever before. As a result, the critical assets of financial institutions are no longer only physical (e.g., bank branches, buildings, ATM machines), but comprise many different cyber assets (e.g., computers, networks, IoT devices) as well. However, the increased digitization and sophistication of the critical infrastructures of the finance sector has also raised the importance of cybersecurity in the finance sector.

Large-scale cyber-attacks on critical financial infrastructure are a major threat, which can cause significant damage and disruption to the financial sector and the wider economy. The complexity of financial services industry, the interconnectedness of individual players and the introduction of new and innovative technologies further increase the risk of a large-scale cyber-attack on the financial sector[1]. Nevertheless, despite significant investments in cybersecurity, system failures are inevitable because the modern financial system is open and therefore more vulnerable to attack.

Aligning investment levels with goals is challenging: this requires scaling up not just overall investment in cybersecurity but also scaling up impact, especially in better harnessing the results of research spending and ensuring the effective targeting and funding of start-ups-SMEs and MEs.

Global spending on cybersecurity is increasing as it becomes difficult to keep up with the rise in cybercrime and malware attacks on governments and organization. The rising importance of cybersecurity in the finance sectors has led banks and financial institutions to invest in cybersecurity solutions and services. This has increased the cyber-resilience of financial actors. As an example the banking, financial services and insurance (BFSI) sector accounts for almost 24% of the global cybersecurity market share in 2020[2]. The global cybersecurity market is expected to exceed USD 330 billion by 2027.

Nevertheless, the situation is more challenging for digital finance SMEs, which typically lack the knowledge and capital needed to develop a proper cyber-defense infrastructure. In this context, digital finance SMEs need to raise their cyber-security awareness, and to deploy Cyber-Security Processes and Tools that can help them improve their cyber-resilience.

Financial SMEs and MEs need a holistic approach that assesses the criticality of their IT infrastructure as a whole, rather than on an ad hoc basis. Following a criticality assessment, SMEs must take measures to segment and isolate critical systems like those engaged in financial transactions in order to properly mitigate risks. Specifically, it is nowadays suggested that risk assessment evolves to take into account the vulnerabilities of multiple assets (e.g., all possible end-points), including their interdependencies and cascading effects of possible attacks. Furthermore, the importance is that SMEs and MEs become aware of methods for analyzing, managing and acknowledging cyber security and data protection risks.

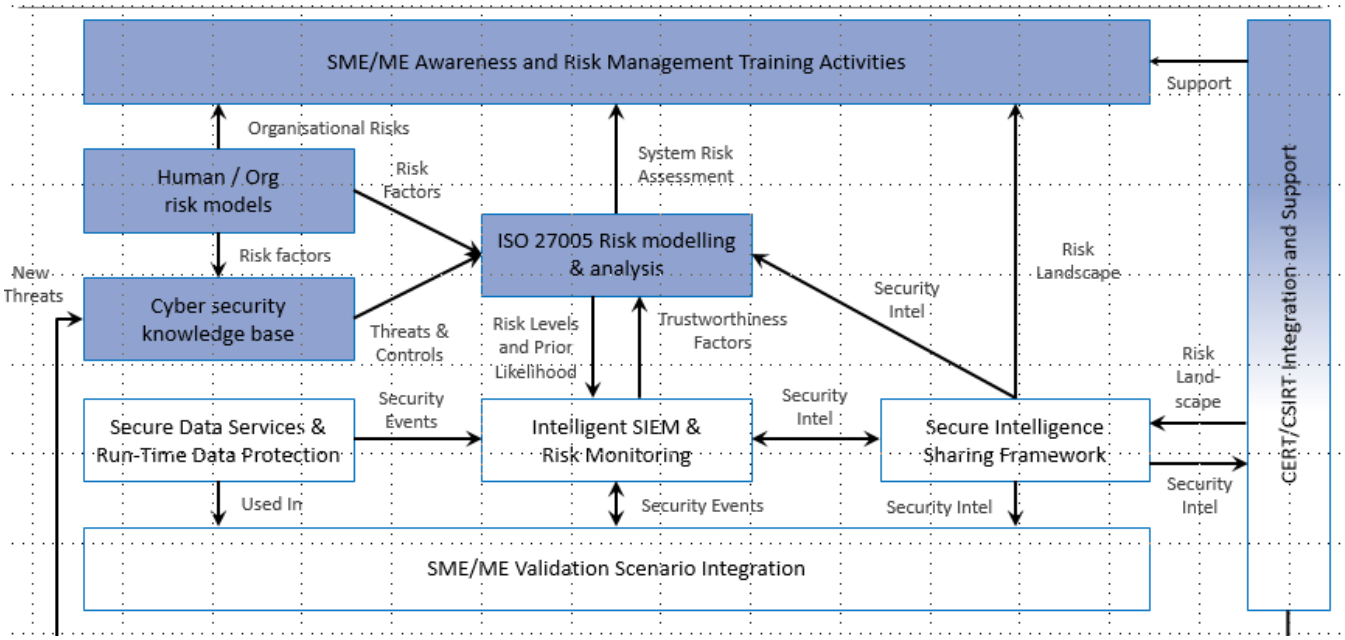
[1] https://www.finextra.com/blogposting/20387/the-state-of-cybersecurity-in-financial-services

[2] https://www.globenewswire.com/en/news-release/2021/11/04/2327215/28124/en/Growth-Opportunities-in-the-Global-Cyber-Security-Market-to-2027-Growing-Cyber-Attacks-and-Remote-Work-Drive-Growth-of-Cybersecurity-Needs-Across-Business-Models.html

CyberKIT4SME: Lowering the Cyber-Resilience Barriers for SMEs

Financial services are at the heart of our global economy and it's safe to say cybercrime is a major risk for the digital finance ecosystem. Cybersecurity has become a vital investment for the financial sector, yet SMEs have not easy and effective ways to understand cybersecurity risks, assess their impact and ultimately mitigating them.

Acknowledging the modern cybersecurity challenges faced by SMEs the CyberKIT4SME project is developing a toolkit that enable small businesses to become more aware of risks so they can monitor, predict and manage them. The project's toolkit provides sophisticated levels of analysis and protection in a low-cost, easy-to-understand and collaborative manner, as well as facilities that support incident reporting and security information sharing and collaboration with other SMEs, larger supply chain partners and security teams like Computer Emergency Response Teams (CERT) and CSIRTs (Computer Security Incident Response Teams).

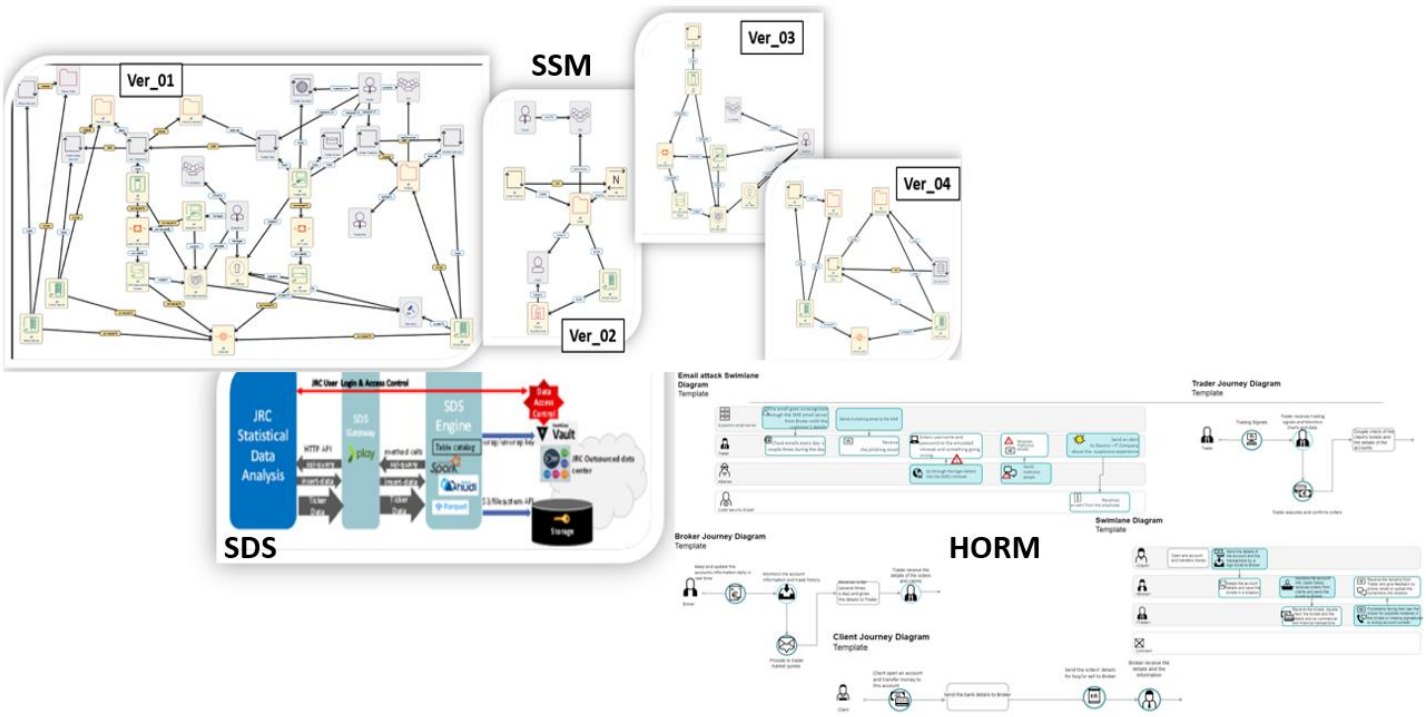


Specifically, CyberKIT4SME offers the following tools:

- System Security Modeler (SSM), which helps SMEs to automate much of their cybersecurity risk assessment. In the digital finance sector, the use of SSM provides vital support, as in addition to scanning for cyber threats it will also check for GDPR compliance.
- Secure Data Services (SDS) are services that protect data throughout its lifecycle as it is stored, accessed and used. This helps SMEs, and the digital finance sector, as it includes facilities to regulate access to and validation of data throughout its lifecycle.
- Human and Organizational Risk Modelling (HORM) is a formal language that helps SMEs to specify and visualize customer/user journeys and service delivery processes. In digital finance sector the use of HORM provides vital support for focusing on people and human activities, regardless of their role of being a customer, employee, user or patient.

JRC Capital Management Consultancy and Research GmbH (https://jrconline.com/) leverages available finance information (e.g., news, trades, alternative data), financial expertise of its personnel, as well as in-house processes and tools, to provide optimal trades for its customers. The added-value of JRC's operations is reflected on the customer's profit. The integrity and protection of the process and of the information exchanged is therefore vital to the company's business continuity and overall success.
JRC benefits from its participation in the **CyberKIT4SME project,** which provides access to a set of user-friendly and easily accessible cybersecurity tools for Small Medium Enterprises. In the scope of the project, JRC has simulated various security scenarios to access the cyber-security risks of the company, to raise cyber security knowledge within JRC's personnel and to identify mitigation actions and plans. Specifically, JRC uses CyberKIT4SME tools in the following ways:

- HORM to model and identify gaps and risks in financial business process and highlight vulnerabilities and risks associated with them. In addition the tool educate users who understand the security implications and risks of their actions and give more robustness in trading processes.
- SDS to encrypt different types of data at different points of their processing pipeline, including: Data received from data providers (e.g., paid trading ticker data) and exported from the trading station for further analysis. Furthermore the use of the Secure Data Service (SDS) tool ensures the integrity and safeguards the intellectual property (IP) of the paid ticker/feed and the company's analytical results.
- SSM is used to assess the major risks faced by the company, to define relevant mitigation actions and back-up solutions and to prioritize the deployment of security controls towards avoiding catastrophic downtimes. SSM tool allows the company to analyze and identify cybersecurity issues at various process levels. Specifically, the SSM tool was used to create a socio-technical model of the assets involved in the transaction process. In addition, the tool includes a simple model of GDPR requirements indicating that the system must provide user interfaces that allow the customer to give consent to the processing of their data, that they are legally capable of giving consent (i.e. not a child), etc.



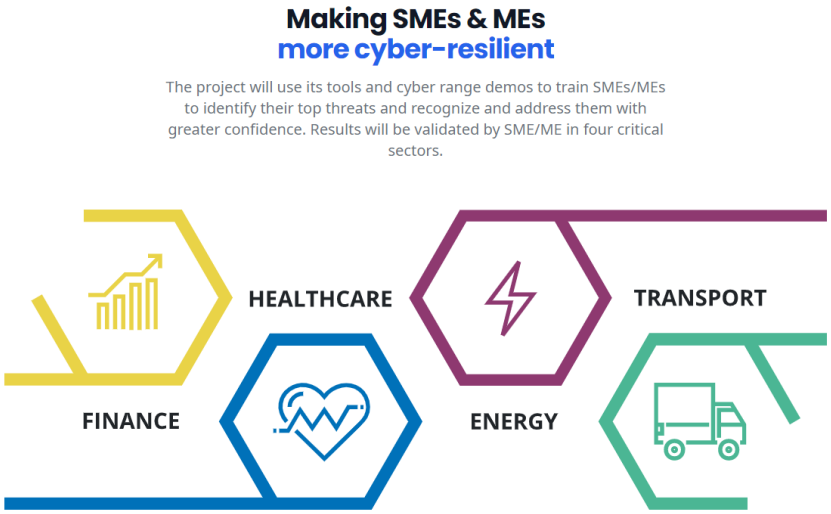
Outlook and More Information

The critical infrastructures of the financial sector are increasing in size, complexity and sophistication, while at the same time comprising both cyber and physical elements. At the same time financial organizations are obliged to comply with many and complex regulations and directives about security, privacy and data protection. As a result, financial enterprises must deal with increased security vulnerabilities and threats in a rapidly evolving regulatory environment. To this end, they are increasing their investments in cybersecurity and its intersection with physical security. Despite the rising investments, they remain vulnerable to security and privacy threats, as evident in several notorious incidents that have occurred during the last couple of years.

In order to properly secure the critical infrastructures for the financial sector there is a need for a new integrated approach that addresses physical and cybersecurity together like the aim of the CyberKIT4SME project. CyberKIT4SME will contribute to create a trustworthy EU digital environment benefitting all economic and social actors by:

- **Helping** SMEs and MEs to become strong links in the cyber security chain underpinning the EU digital environment.
- **Improving** the security of SME-ME services, data and infrastructures.
- **Strengthening** security, privacy and personal data protection.
- **Reducing** the damage caused by cyber-attacks and data protection breaches.

JRC is using these tools to improve the cyber-security awareness of its personnel, but also to assess and mitigate risks associated with its processes. We are also benefitting from encrypting sensitive data to avoid data breaches and to safeguard our own and our customers' Intellectual Property.



For more information on CyberKit4SME: https://cyberkit4sme.eu/

Follow us on Twitter: https://twitter.com/CyberKit4SME

Follow us on LinkedIn: https://www.linkedin.com/company/cyberkit4sme?trk=public_post_share-update_actor-text

Contact us at: https://cyberkit4sme.eu/contact-us/ or email: info@cyberkit4sme.eu