Finance Sector: Awareness, Assessment and Mitigation in Cybersecurity

H2020 CyberKIT4SME Project

https://cyberkit4sme.eu/

JRC Capital Management and Consultancy GmbH Berlin, Germany

1. Significance of Cybersecurity in Digital Finance Sector

In the dynamic landscape of the financial sector, the imperative role of cybersecurity cannot be overestimated, especially with regard to safeguarding critical assets and the particular challenges faced by Small and Medium Enterprises (SMEs) and Micro Small Enterprises (MSMEs). In the financial sector, which is increasingly dependent on digital infrastructure, critical assets include highly sensitive data such as customer data, transaction records and vital financial information, such as customer data, transaction logs and financial information. Preserving these assets is paramount to ensure trust and the overall stability of the industry.

SMEs and MEs operating in the financial sector often face limited resources and limited expertise, making them vulnerable targets for cyber threats. Increasing their defensive capabilities and enhancing their cyber resilience are fundamental imperatives. Recognizing the pivotal role that SMEs and MEs play in the wider financial ecosystem, this calls for an unwavering commitment to strengthening cybersecurity practices. By prioritizing the protection of critical assets and making prudent investments in cybersecurity measures, both prominent financial institutions and SMEs and MEs can collectively contribute to fostering a more robust, secure financial sector that adeptly adapts to the progressively digital landscape.

Financial SMEs and MEs should evaluate the criticality of their IT infrastructure holistically, rather than on an as-needed basis. The company should take the appropriate steps to divide and isolate vital systems, such as those involved in financial transactions, after conducting a criticality evaluation. In particular, it is currently recommended that risk assessment develops to consider the vulnerabilities of many assets (i.e., all potential endpoints), including their interdependencies and the potential for assaults to cascade into one another. Additionally, it is critical that SMEs and MEs understand, assess, control, and recognize the risks associated with data protection and cyber security.

2. Solving problems related to the digital financial sector with the CyberKIT4SME Project.

Financial services are at the heart of our global economy and it is safe to say cybercrime is a major risk for the banking system. Cybersecurity has become a vital investment for the financial sector.

The continued digitization of financial services, the obsolescence of certain banking information systems and the interconnection with third-party information systems and, by extension, migration to the cloud are the main risks that need to be addressed.

With regard to the financing sector, there are specific characteristics that make cyber-attacks very serious, both in terms of the likelihood of occurrence and the potential severity of the impact. **Data security is a major issue for the financial sector, which plays a key role in the economy**. A security incident in a banking institution can have consequences on the day-to-day operations of an entire country, or even an entire region of the world. Today's financial services are entirely dependent on computer systems. Although they started to digitalize very early on – today, lots of information systems (IS) are obsolete. In fact, many security incidents have been linked back to maladjusted tools. In some cases, software patches simply aren't installed[1].

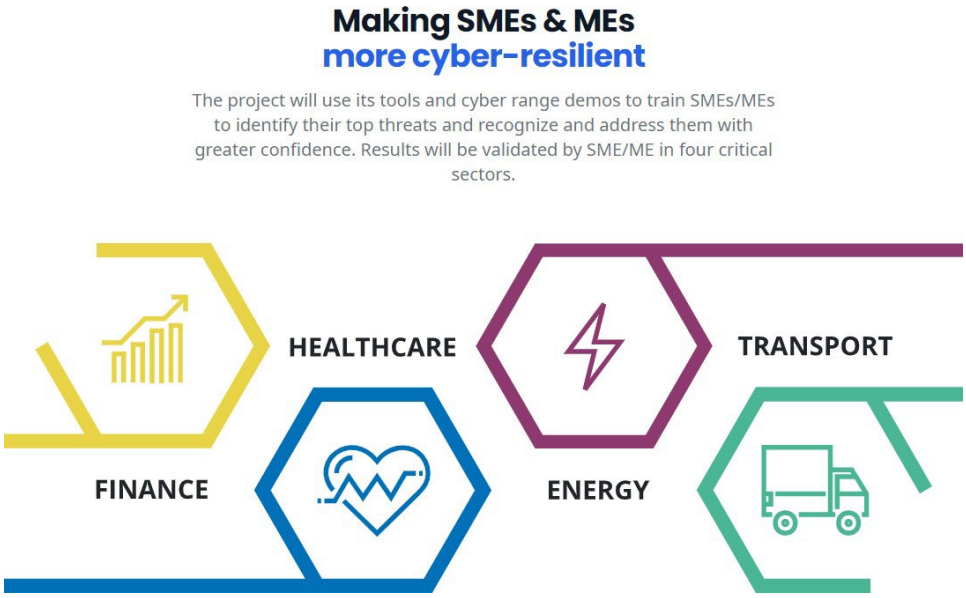
Taking a step towards in this direction, the CyberKIT4SME project is developing tools that will enable small businesses to become more aware of risks so they can monitor, predict and manage them. The toolkit will provide sophisticated levels of analysis and protection in a low-cost, easy-to-understand 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 CERT/CSIRTs.

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. Cybersecurity is becoming a strategic imperative for the organization due to the increased focus on preventing information in the wake of theft and high-profile data security. Global spending on cybersecurity is increasing as it becomes difficult to keep up with the rise in cybercrime and malware attacks on governments and organizations. The adoption of cybersecurity solutions is expected to increase with the growing internet penetration between developing and developed countries. Also, the expansion of wireless network for mobile devices has increased the vulnerability of data making cybersecurity an integral part of every organization.

Conclusion

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 H2020. CyberKIT4SME H2020 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



[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