Cybersecurity Blueprint for Finance SMEs

H2020 CyberKIT4SME Project -White Paper

September 2023

https://cyberkit4sme.eu/

Konstantina Tripodi

Rico Ehmke

JRC Capital Management and Consultancy GmbH Berlin, Germany

Finance SMEs and Cybersecurity: an introduction

In an increasingly digital world, Small and Medium Enterprises (SMEs) in the finance sector are often targeted by cyberattacks due to their perceived lower levels of protection. A robust cybersecurity blueprint would help these entities to safeguard their assets against cyber threats.

The finance sector SMEs should start conducting regular risk assessments and manage any identified potential cyber risks within the organization. This helps pinpoint vulnerabilities and weak points in their digital systems that could be exploited as breaches. In addition, implementing robust cybersecurity measures, such as firewalls and secure servers, can reinforce the organization's defenses. Utilizing intrusion detection and prevention systems can thwart potential threats early on. Encrypting sensitive data adds a layer of protection even if a breach occurs. Finally, a secure network design using Virtual Private Networks (VPNs) for remote access and segmenting the company network into different zones can not only further enhance control and security, but also reduce damages in case of successful attack.

It is essential to regularly update systems, applications, and security tools since timely software patching reduces attack chances. Equally important is employees training so they understand the importance of cybersecurity, can identify and avoid social engineering attacks, and know to report suspicious activities.

Preparing an effective incident response plan is crucial, outlining the steps to be taken in case a cybersecurity incident occurs, thus facilitating a swift response and recovery from cyberattacks. Regular audits, including penetration tests and vulnerability assessments, can identify potential security gaps, while reliable data backup procedures and a robust disaster recovery plan ensure business continuity even in case of a cyberattack breach. Financial SMEs should carefully evaluate the security protocols of any third-party vendors before integrating their systems and continuously assess their own systems' compliance with industry regulations and standards for cybersecurity. In essence, cybersecurity for finance SMEs should not be viewed as a one-off task, but a continuous process involving regular risk assessment, maintaining and updating protection measures, timely detection, and response to threats, while staying informed with fast-evolving cybersecurity technology and the always evolving cyberthreats landscape.

Potential Cybersecurity Exploitable Assets in the Financial Sector

The advanced digitization of the financial sector, while driving operational efficiency and growth, has unfolded a series of assets that are potentially susceptible to cyber threats.

1. Data Repositories: given the sensitivity and value of the information they hold, data centers of financial institutions become lucrative targets for cybercriminals aspiring to access personal, corporate, and financial data.

2. IT Infrastructure: the networks and systems of financial institutions, accessed and used by finance SMEs, deployed for daily transactions, data storage, processing, and communication are high-priority targets for cyber attackers.

3. Digital Interfaces: the increasing prominence of digital banking implicates mobile apps and online platforms in a heightened risk of cyberattacks. These platforms provide access to a large number of user accounts and handle significant transaction volumes, thereby inviting exploitation.

4. Transaction Channels: Systems involved in payment processing like credit card networks, digital wallets, and wire transfer mechanisms attract cyber threats due to the substantial monetary flows they facilitate.

5. Software Solutions: Diverse software applications, ranging from transaction processing systems to customer relationship management tools, employed within the financial sector can be readily exploited in cases of any inherent bugs or vulnerabilities.

6. Human Elements: Employees or internal resources can be manipulated via social engineering attacks geared towards unauthorized information or systems access.

7. Outsourced Vendor Systems: Financial institutions often depend on third-party vendors for specialized services. Should these vendors lack adequate security measures, their systems could potentially provide cybercriminals a back-door entry.

8. Cloud Solutions: With cloud-based services increasingly being adopted by financial institutions, these can become points of exploitation if their security protocols are not sufficiently robust.

9. BRING YOUR OWN DEVICES (BYOD) in organizations brings security risks, including malware and data breaches. Employees' personal devices may lack strong security, leading to unauthorized access and weak password practices. Control over personal devices is limited, making policy enforcement challenging. Inadequate updates and data mixing further compound risks. To mitigate, consider Mobile Device Management, employee training, strong authentication, clear BYOD policies, regular monitoring, and data separation. Keeping devices up-to-date is crucial for security. Overall, BYOD offers flexibility but requires robust security measures to protect against potential threats and data compromise.

In recognition of these potential exploitable and precious assets, implementing strong cybersecurity measures to secure them can contribute substantially in protecting the financial sector from crippling cyber-attacks.

Future Perspective and Additional Insights

The critical infrastructures within the financial sector are experiencing progressive growth in their scale, intricacy, and advancement, seamlessly integrating both cyber and physical aspects. Concurrently, financial institutions must adapt to an array of multifaceted regulations and guidelines related to security, privacy, and data protection. It compels these organizations to mitigate escalated security vulnerabilities and impending threats within a dynamically changing regulatory realm. Their proactive counteraction has led to a substantial increase in investments aimed at reinforcing cybersecurity and its interplay with physical security. Nevertheless, rising investments have not entirely dispelled the susceptibility to security and privacy threats, as multiple high-profile incidents in recent years have illustrated.

Safeguarding the critical infrastructures within the financial sector necessitates an innovative, integrated strategy that synchronizes the interplay between physical and cybersecurity dimensions, a strategy encapsulated within the mission of the CyberKIT4SME research project, co-funded by the European Union. The CyberKIT4SME partnership aims to play a pivotal role in establishing a dependable digital landscape throughout Europe, conferring benefits upon diverse economic and societal entities. The core objectives driving the CyberKIT4SME venture are:

1. Facilitation of resilience-building among Small & Medium Enterprises (SMEs) and Medium Enterprises (MEs), enabling them to become robust constituents in the cybersecurity chain fortifying the EU’s digital infrastructure.

2. Enhancement of the security protocols central to SMEs' services, data management, and overall infrastructural integrity.

JRC Capital Management (JRC), as partner of the CyberKit4SME consortium, is using these tools to improve the cyber-security awareness of its personnel, but also to assess and mitigate risks associated with its processes. JRC is also benefitting from encrypting sensitive data to avoid data breaches and to safeguard its own and its 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

CyberKIT4SME Brochure

1 June 2020 – 31 May 2023

CyberKit4SME Partners:

inetum
Positive digital flow

Elektrobit
TIANI SPIRIT
University of Southampton
IBM
Energis
3SOFT
SINTEF
sogei
jrc CAPITAL MANAGEMENT

EU Horizon H2020 Call
SU-DS03-2019-2020

Digital Security and privacy for citizens, Small and Medium Enterprises and Micro Enterprises

Budget: 4,890,725€

Contact:
cyberkit4sme.eu
info@cyberkit4sme.eu

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883188.

CYBERKIT 4SME

Democratizing a Cyber Security Toolkit for SMEs and MEs

Cyberkit4sme.eu

CyberKit4SME:

Making SMEs more cyber-resilient

The EU-funded CyberKit4SME project will develop tools to enable small businesses to become more aware of the risks so as to monitor, forecast and manage them. Specifically, it will design affordable and easy-to-use encryption and isolation tools to protect data. Blockchain tools will also be advanced to enable SMEs to share intelligence and incident reports with computer emergency response teams.

Scope and objectives

CyberKit4SME aims to democratize a kit of cyber security tools and methods enabling SMEs/MEs to:

- Increase awareness of cybersecurity risks, vulnerabilities and attacks;
- Monitor and forecast risks;
- Manage risks using organisational, human and technical security measures with greater confidence;
- Collaborate and share information in a collective security and data protection effort.

Methodology and Innovative Tool

- Offline risk modelling tools to support ISO 27005 risk analysis and privacy and data-protection 'by design'.
- Online cyber security risk monitoring based on collaborative security intelligence and event management (SIEM) tool.
- Cyber security incident reporting and security intelligence sharing support by a secure, privacy-aware blockchain framework, allowing SMEs to collaborate with CERTs, supply chain partners and other SMEs.

The project will use its tools and cyber range demos to train SMEs/MEs to identify their top threats and recognise and address them with greater confidence. Results will be validated by SME/ME in four critical sectors: Finance, Health Care, Energy and Transport.

Impact

CyberKit4SME will contribute in creating a trustworthy EU digital environment benefitting all economic and social 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.

CyberKit4SME aims to help SMEs and MEs demonstrate compliance with any regulation that imposes requirements for cyber security or data protection.