

Networks and Cyber Security Essentials
ACCA4024

Shaun James Davies
2317135

Word Count:

1834

Table of Contents

I.	INTRODUCTION.....	3
II.	IDENTIFICATION OF THREATS	3
A.	INTERNAL THREATS.....	3
B.	EXTERNAL THREATS	3
III.	SECURITY POLICIES	4
IV.	MITIGATION MEASURES	4
A.	INTERNAL THREATS	4
1)	<i>Weak Access Controls</i>	<i>4</i>
2)	<i>Insider Threat.....</i>	<i>5</i>
3)	<i>Inadequate User Awareness</i>	<i>5</i>
B.	EXTERNAL THREATS.....	5
1)	<i>Social Engineering.....</i>	<i>5</i>
2)	<i>Malware and Ransomware</i>	<i>5</i>
V.	MONITORING AND RESPONSE	5
A.	MONITORING TOOLS.....	5
1)	<i>Intrusion Detection/Prevention Systems (IDS/IPS).....</i>	<i>5</i>
2)	<i>Endpoint Detection and Response (EDR)</i>	<i>5</i>
3)	<i>Email and web filters.</i>	<i>5</i>
B.	INCIDENT RESPONSE PLAN	5
VI.	TRAINING AND AWARENESS.....	6
VII.	CONCLUSION	6
	APPENDIX.....	7
	REFERENCES	13

FinSecure Ltd Cybersecurity Solution

Abstract –

Cybersecurity is a rising concern for businesses globally. This report is a tailored set of cybersecurity best practices and policies to ensure a reduced risk of threats causing damage to the company.

Comparing 2012 figures to 2022 this trend has reversed [1]. Although, to provide a comprehensive CS prevention plan both threats need to be considered.

I. INTRODUCTION

Cybersecurity (CS) is globally recognised and due to only grow in prominence for companies, namely financial companies. The prevalence of cybercrime across the globe ensures that CS of devices and systems remains at the forefront of company interests. The growth between both crime and security is set to continue as every entity involved, company and criminal, aim to best the other to either protect or steal company data, assets and resources.

Attack vectors are increasing, with the rise of remote work. Tablets and other personal devices increase the CS challenges faced by companies. An increasing pressure on companies is present to ensure IT managers, policy makers and all stakeholders understand their role in business CS. Without a holistic and up to date approach to CS internal and external threats and attack tactics will best weakened and outdated company approaches. FinSecure Ltd (FSL) has faced phishing attacks and unauthorised access attempts. The company requires the correct and up to date approach to CS with relevant standards, policies, and current literature enforcing and leading the design, creation and implementation of a unique FSL CS policy to mitigate internal and external threats. Throughout this report, a clear, relevant and effective demonstration of tailored advice will be displayed.

A myriad of up to date information sources have been gathered to:

- Explore threat identification
- Develop security policy
- Demonstrate mitigation measures
- Highlight monitoring and response plans
- Produce aware employees with staff training programs.

II. IDENTIFICATION OF THREATS

A variety of threats can face a financial company. Internal and external threats are possible from political, economic, social, technological, legal and environmental vectors.

External threats consist of a large majority of recent years of cyber-attacks. In previous years, internal “insider” threats have proven to be a bigger threat.

A. Internal threats

- Weak Access controls is a common threat to CS [2]
- Unsecured devices and remote access [3].
- System error and flaws [4]. By “systematically reviewing and rigorously analysing the literature on software security patch management” this threat can be reduced or eliminated [5].
- Malicious insiders and other insider threats: employees or otherwise insiders can harm the organisation for personal gain [6].
- Exploitation of privileged access: to mitigate risk a policy for user access is essential [6].
- Inadequate user awareness: a lack of training for employees leaves them unequipped to observe occurring security threats from a lack of awareness, knowledge and skills [6].

B. External threats

- Social engineering: FSL should consider this attack vector that affects the “physical, technical, social and socio-technical dimensions” [1]. This threat is the initial cause of “security breaches” [7].
- Phishing attacks: as this threat has influenced the company previously, this is an attack vector. This is when an email deceives an employee at any level of the company to, unbeknownst to the victim, reveal company credentials or enter online links through the email. These fake emails can appear from the company or otherwise legitimate. This can cause damage to the company, customer and data systems and is “based on social engineering” [8].
- Malware and Ransomware: software that can watch, manipulate or mimic user activity. It can view data, encrypt files with unknown passwords and even hold data ransom over the customer or company. In recent years, companies like FSL and others in the financial sector

- Distributed Denial of Service (DDoS) attacks: DDoS overloads company systems with traffic which can cause service outages and is prominent in the current climate [9]. The aim for these attacks are to pause or stop operations, break customer trust with system outage and can be an initial attack to weaken or otherwise disrupt systems.
- Third-party vulnerabilities: FSL may rely on other companies for their services. Poorly maintained CS from these companies can indirectly cause data loss which can “compromise considerably larger amounts of data” [10].

Figure 1 displays eleven donut charts, each representing a different type of cyberattack. Each chart is divided into six segments, representing different sectors: Government, Financial, Health, Education, Energy, and ICTs. The sectors are: 1. Malware Attacks, 2. DDoS Attacks, 3. Social Engineering, 4. Insider Attacks, 5. Data Leak, 6. Data Breach, 7. Internet Fraud, 8. Industrial Espionage, 9. Power Attacks, 10. Digital Extortion, and 11. Vulnerabilities in IoT.

III.SECURITY POLICIES

The policies listed in Table 1 should be implemented in the following order of importance. The company policies should include four aspects, and each policy should pair with at least one.

- [4]

IV.MITIGATION MEASURES

To reduce the aforementioned threats at FSL the following measures should be implemented as part of the CS plan.

A. Internal Threats

1) Weak Access Controls

Table 1 A comparison of the themes against Patrick's present in this paper										
Rank	Name of theme	References	# Pages	Targets	Medications	Threats against attack	Disturbance level	HPV	Main platform	Special Attention
1	Machine	Black et al., 2016; Fieser et al., 2015; Pichler-Lapin & Martin, 2017	3	Operating centers	Machine destruction	3	●	●	Network, Possible	Automated
2	AI Attacks	Grims et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	4	Network	Service disruption, Denial of service	3	●	●	Network	Automated
3	Digital AI	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	4	Network	Service disruption, Denial of service	3	●	●	Web	Hybrid
4	Infected	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	4	Industrial control	Service disruption, Denial of service	3	●	●	ICS	Automated
5	Industrial	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Industrial control	Technology theft	3	●	●	ICS	Automated
6	Industrialization	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Industrial control	Service disruption, Denial of service	3	●	●	ICS	Automated
7	Power Attacks	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Power agencies	Flawed grid, Denial of service	3	●	●	Power	Automated
8	Attack Attacks	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Any thing	Flawed, Denial of service, and tampering	3	●	●	Any	Manual
9	Engineering	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Any thing	Flawed, Denial of service, and tampering	3	●	●	Any	Manual
10	Control	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Any thing	Flawed, Denial of service, and tampering	3	●	●	Web	Hybrid
11	Discrete Load	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Any thing	Information gathering	3	●	●	Control channels	Hybrid
12	Discrete Load	Black et al., 2016; Houghton et al., 2015; Maleski & Haddad, 2017	3	Any thing	Information gathering	3	●	●	Web	Hybrid

A pie chart illustrating the distribution of security incidents. The chart is divided into eight segments of varying sizes and colors, each labeled with an incident type and its corresponding percentage. The segments are: Malware (28.92%, brown), Misuse by staff (26.51%, pink), Threats related to vendors, third-parties, freelancers (21.69%, green), Breaches by hackers (12.05%, blue), DDoS attacks (4.82%, light blue), Phishing (3.61%, yellow), Smart card driver error causing RDS server crash (1.20%, grey), and C&C bot activity (1.20%, orange).

Incident Type	Percentage
Malware	28.92%
Misuse by staff	26.51%
Threats related to vendors, third-parties, freelancers	21.69%
Breaches by hackers	12.05%
DDoS attacks	4.82%
Phishing	3.61%
Smart card driver error causing RDS server crash	1.20%
C&C bot activity	1.20%

Fig. 2. Further Threats to CS pie chart by percentage [3].

beings are the weakest link in the digital system's life cycle" [1]. highlighting how crucial it is to concentrate on educating staff members on how to recognise and handle security issues. Frequent security awareness training ought to be a top concern.

2) Insider Threat

Stressing the increased danger of insider attacks is crucial, as it highlights the necessity of creating thorough pre-employment, during employment, and post-employment rules for workers, contractors, and other workers. "Post-employment has been the most neglected policy in many big companies" [1]. Monitoring privileged access and putting strong confidentiality agreements into place are crucial.

3) Inadequate User Awareness

FSL should make an investment in a "cyber-culture" that incorporates security knowledge at all organisational levels, since human mistake frequently leads to security breaches. The source emphasises that "cyber-culture and security awareness was recognised as the most effective solution," which involves regular CS training that addresses both technological and human dangers [1].

B. External Threats

1) Social Engineering

This attack vector exploits human weaknesses. According to the paper, all staff members should participate in "comprehensive CS training programs" to get a greater awareness of attack vectors [1]. The detection of questionable emails, phone calls, and other electronic communications should be the main goal of awareness campaigns.

2) Malware and Ransomware

The employment of hybrid malware analysis techniques and strong anti-malware software is crucial to this CS strategy for FSL because malware attacks are on the rise. Additionally, it recommends using frequent server data backups to reduce ransomware impact [1].

By incorporating these recommendations and the defences from Fig.4. into FSL's CS policies, internal and external threats can be effectively mitigated, enhancing the CS of the organisation.

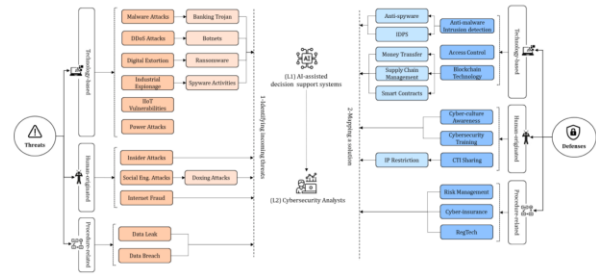


Fig. 4. Threats and the required defences [1].

V. MONITORING AND RESPONSE

FSL will put in place a centralised Security Information and Event Management (SIEM) system that will gather, examine, and correlate log data from several sources, including firewalls and endpoints, on a continuous basis. By facilitating "real-time behavioural anomaly detection" and "faster incident management," SIEM systems give users insight into possible dangers. FSL's proactive security measures and compliance will be strengthened by complementary tools like IDS/IPS, EDR, and email/web filters, which will further improve detection of suspicious activities including malware, unauthorised access, and phishing [13].

A. Monitoring tools

1) Intrusion Detection/Prevention Systems (IDS/IPS)

For "monitoring the events occurring in a computer system or network" [14] to ensure adherence to policy.

2) Endpoint Detection and Response (EDR)

This is a tool for suspicious activity across "multiple hosts" to analyse end point with "deep insight" [15].

3) Email and web filters.

To flag phishing and malicious content [12].

B. Incident Response Plan

As detailed in Fig. 5., the following steps discuss the incident response plan required for FSL.

Step one is the detection stage of the plan. This is to prepare, detect and receive alerts from monitoring tools assessed effectively by security analysts.

Step two is "respond" and containment which entails sectioning devices or systems to prevent further damage to other systems and prevent spread.

Step three is eradication which, once correctly identifying and removing the threat, is used to determine the root cause of the CS breach.

Step 4 is recovery which restores systems from backups and tests are carried out to ensure the backups are clean.

The final step, step 5, is a post threat analysis or “lessons learned” which is used to focus on how to improve CS aspects of the business from this threat [16].

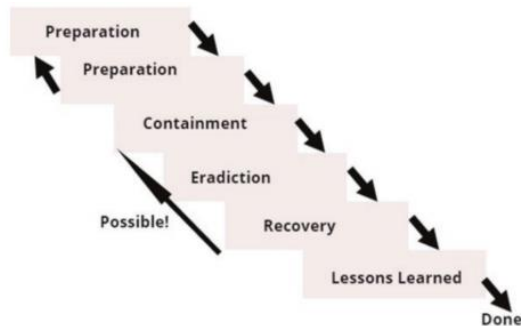


Fig. 5. Incident response flow [16]

VI. TRAINING AND AWARENESS

CS skills and skilled people have faced a “critical level of shortage”. Despite training being a “time-consuming task” it can lead to improved CS within the company [1].

An important part of every CS approach is awareness and is “the most important missing part in FinTech services [1]. To ensure compliance with FSL’s security policies, all staff will undergo mandatory CS training. New employees will receive onboarding sessions covering core topics like password policies, phishing, and acceptable use. Monthly microlearning modules and quarterly phishing simulations will reinforce learning. Staff in sensitive roles (e.g., IT, Finance) will receive tailored training. Policy acknowledgments will be required after major updates.

VII. CONCLUSION

Demonstrated throughout this report, providing financial companies with a comprehensive CS approach is vital for business continuity and function through a dynamic cyber threat landscape. FSL previously expressed difficulty with attack vectors and was at risk of financial, business, operational, reputational and legal damages and consequences. By implementing this comprehensive FSL CS holistic policy CS threats can be minimised, reduced and otherwise mitigated.

Internal threats such as weak access controls, unsecured devices, system errors and insider threats have been identified and detailed. External threats

including social engineering, phishing attacks, malware, ransomware, DDoS attacks, and third-party vulnerabilities were considered whilst forming the unique FSL CS approach. Aligning to industry standards and best practices ensures strong foundations to FSLs security framework.

By including effective mitigation measures, monitoring and response plans, security incidents are minimised and so is the potential damage to the company. This damage is typically caused by employees more often than system issues. Empowering employees with adequate learning and security awareness can reduce the likelihood of an incident occurring improving the CS posture of the company.

APPENDIX

Table 1:

No.	Policy	Importance Explanation	Controls	Aspect
1	Password and Authentication [8]	Weak passwords can lead to unauthorised access and to breaches. This has been an issue for FSL previously so it's required.	Length and complexity rules i.e. 8 or more character with special characters and no names.	Technical and physical – unauthorised access attempted on FSL have occurred.
2	Email and Communication [8]	Phishing attacks are reported attack vectors. Communication policies can prevent future cases.	Email filters to flag phishing emails and train employees in identifying threats.	Personal resilience – teaches employees to avoid and report social engineering attacks.
3	Access Control [8]	Reduces access to those who require it only to do their job and nothing more.	Role based access with defined roles for each employees.	Technical and physical – limits exposure of technical and sensitive data.
4	Remote Work [3]	Ensures correct and authorised access to company hardware systems from remote locations and personal equipment.	Virtual private networks (VPNs) allow for protected remote access. Personal devices should meet minimum security standards such as antivirus.	Technical and physical – Supports work from home environments
5	Incident Reporting [17]	Encourages employees to report cybersecurity incidents such as data breaches and malware.	Create an employee cybersecurity incident reporting system or call centre.	Personal resilience – builds staff accountability and early threat detection.
6	Acceptable Use (AUP) [8]	Restricts employees and sets guidelines on IT usage and sets boundaries so that employees only use work devices for work purposes.	Restrict use of USBs and unapproved hardware. Prohibit software. Monitor usage	Organisational measures – creates expected behaviour and system boundaries for employees
7	Patch Management [8]	Regularly update software to protect against vulnerabilities.	Automate patching for operating systems.	Technical and physical – prevents flaws from becoming attack vectors.
8	Data Classification and Handling [18]	Ensures employees define data, files and other documents. Then specify handling procedures for each definition.	Use public, internal, confidential and restricted tags to each file. Encrypt sensitive data. Access control to be placed on files based on classification.	Organisational measures – creates expected behaviour and system boundaries for employees

9	Network Security [19]	Focuses on firewalls, intrusion detection and other network security.	Implement firewalls, network monitoring tools and regularly test vulnerability.	Technical and physical – resilience can be build from the foundation of the IT systems.
10	Backup and Recovery [8]	Set up data backups on occasional cycles to ensure business function is maintained if data is lost through an attack.	Set up weekly backups of databases and data systems. Store these back-ups online and on the cloud	Organisational measures – maintains business continuity after cybersecurity incident.

Presentation:



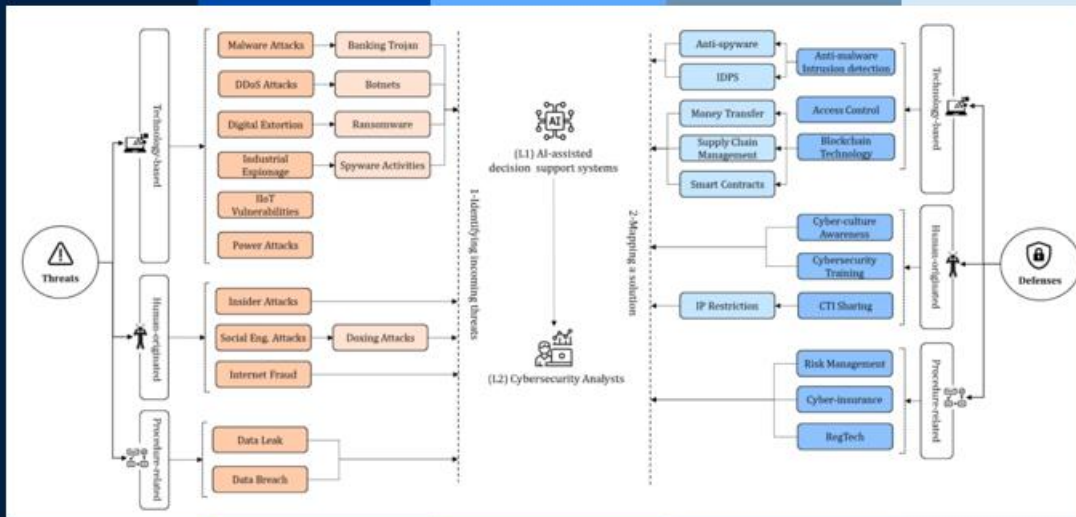
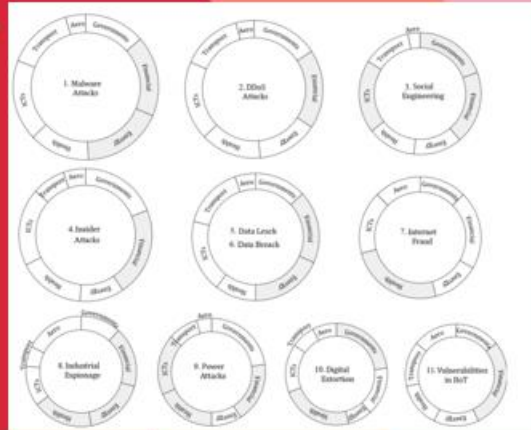
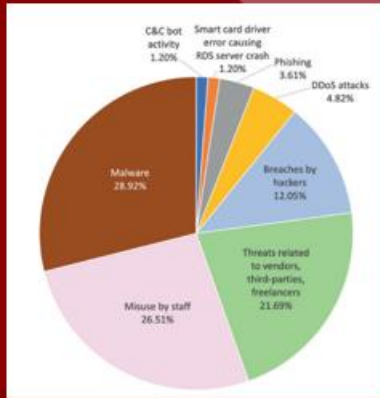
Internal threats

- Weak Access controls is a common threat to CS [2]
- Unsecured devices and remote access [3].
- System error and flaws [4]. By “systematically reviewing and rigorously analysing the literature on software security patch management” this threat can be reduced or eliminated [5].
- Malicious insiders and other insider threats: employees or otherwise insiders can harm the organisation for personal gain [6].
- Exploitation of privileged access: to mitigate risk a policy for user access is essential [6].
- Inadequate user awareness: a lack of training for employees leaves them unequipped to observe occurring security threats from a lack of awareness, knowledge and skills [6].

External threats

- Social engineering: FSL should consider this attack vector that affects the “physical, technical, social and socio-technical dimensions” [1]. This threat is the initial cause of “security breaches” [7].
- Phishing attacks: as this threat has influenced the company previously, this is an attack vector. This is when an email deceives an employee at any level of the company to, unbeknownst to the victim, reveal company credentials or enter online links through the email. These fake emails can appear from the company or otherwise legitimate. This can cause damage to the company, customer and data systems and is “based on social engineering” [8].
- Malware and Ransomware: software that can watch, manipulate or mimic user activity. It can view data, encrypt files with unknown passwords and even hold data ransom over the customer or company. In recent years, companies like FSL and others in the financial sector account for “19% of the total number of malware attacks” which indicate a need to evaluate this threat [1].
- Distributed Denial of Service (DDoS) attacks: DDoS overloads company systems with traffic which can cause service outages and is prominent in the current climate [9]. The aim for these attacks are to pause or stop operations, break customer trust with system outage and can be an initial attack to weaken or otherwise disrupt systems.

Third-party vulnerabilities: FSL may rely on other companies for their services. Poorly maintained CS from these companies can indirectly cause data loss which can “compromise considerably larger amounts of data” [10].





**All key aspects of a
cybersecurity plan**

INCIDENT RESPONSE

MITIGATING MEASURES

MONITORING & RESPONSE

**FSL SUGGESTED
POLICIES**

No.	Policy	Importance Explanation	Controls	Aspect
1	Password and Authentication [8]	Weak passwords can lead to unauthorised access and to breaches. This has been an issue for FSL previously so it's required.	Length and complexity rules i.e. 8 or more character with special characters and no names.	Technical and physical – unauthorised access attempted on FSL have occurred.
2	Email and Communication [8]	Phishing attacks are reported attack vectors. Communication policies can prevent future cases.	Email filters to flag phishing emails and train employees in identifying threats.	Personal resilience – teaches employees to avoid and report social engineering attacks.
3	Access Control [8]	Reduces access to those who require it only to do their job and nothing more.	Role based access with defined roles for each employees.	Technical and physical – limits exposure of technical and sensitive data.
4	Remote Work [3]	Ensures correct and authorised access to company hardware systems from remote locations and personal equipment.	Virtual private networks (VPNs) allow for protected remote access. Personal devices should meet minimum security standards such as antivirus.	Technical and physical – Supports work from home environments
5	Incident Reporting [17]	Encourages employees to report cybersecurity incidents such as data breaches and malware.	Create an employee cybersecurity incident reporting system or call center.	Personal resilience – builds staff accountability and early threat detection.
6	Acceptable Use (AUP)	Restricts employees and sets guidelines on IT usage and sets boundaries so that employees only use work devices for work purposes.	Restrict use of USBs and unapproved hardware. Prohibit software. Monitor usage	Organisational measures – creates expected behaviour and system boundaries for employees
7	Patch Management [8]	Regularly update software to protect against vulnerabilities.	Automate patching for operating systems.	Technical and physical – prevents flaws from becoming attack vectors.
8	Data Classification and Handling [18]	Ensures employees define data, files and other documents. Then specify handling procedures for each definition.	Use public, internal, confidential and restricted tags to each file. Encrypt sensitive data. Access control to be placed on files based on classification.	Organisational measures – creates expected behaviour and system boundaries for employees
9	Network Security [19]	Focuses on firewalls, intrusion detection and other network security.	Implement firewalls, network monitoring tools and regularly test vulnerability.	Technical and physical – resilience can be build from the foundation of the IT systems.
10	Backup and Recovery [8]	Set up data backups on occasional cycles to ensure business function is maintained if data is lost through an attack.	Set up weekly backups of databases and data systems. Store these back-ups online and on the cloud	Organisational measures – maintains business continuity after cybersecurity incident.

REFERENCES

- [1] M. F. H. C. P. L. Danial Javaheri, "Cybersecurity threats in FinTech: A systematic review," *Expert Systems with Applications*, vol. 241, no. 1, pp. 1-31, 2024.
- [2] S. U. K. M. N. M. H. N. U. S. A. K. & A. A. Asif Iqbal, "Advancing database security: a comprehensive systematic mapping study of potential challenges," *Wireless Networks*, vol. 30, no. 7, p. 6399, 2024.
- [3] J. Sabin, "The future of security in a remote-work environment," *Network Security*, vol. 2021, no. 10, pp. 15-17, 2021.
- [4] I. B. Andrei PETROIA, "THE RISKS OF CYBERSECURITY OF FINANCIAL INSTITUTIONS AND POSSIBLE METHODS FOR THEIR ELIMINATION," *INFORMATICS, STATISTICS AND ECONOMIC CYBERNETICS*, vol. 4, no. 110, pp. 156-163, 2019.
- [5] A. J. M. Z. M. A. B. Nesara Dissanayake, "Software security patch management - A systematic literature review of challenges, approaches, tools and practices," *Information and Software Technology*, vol. 144, no. 1, p. 16, 2022.
- [6] E. O. S. O. O. A. a. A. A. Uchenna Joseph Umoga, "A critical review of emerging cybersecurity threats in financial technologies," *International Journal of Science and Research Archive*, vol. 11, no. 1, pp. 1810-1817, 2024.
- [7] T. R. a. N. K. J. a. S. T. a. A. A. a. D. G. a. A. Singh, "A comprehensive survey on social engineering attacks, countermeasures, case study, and research challengesInformation Processing & Management," *Information Processing & Management*, vol. 62, no. 1, p. 103928, 2025.
- [8] B. N. a. K. P. a. A. F. a. I. M. a. S. O. a. J. Porras, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers & Security*, vol. 132, pp. 1-18, 2023.
- [9] A. B. { . N. a. B. K. a. M. Nogueira, "Distributed denial of service attack prediction: Challenges, open issues and opportunities," *Computer Networks*, vol. 222, no. 1, p. 1, 2023.
- [10] M. Benaroch, "Third-party induced cyber incidents—much ado about nothing?," *Journal of Cybersecurity*, vol. 7, no. 1, p. 13, 2021.
- [11] A. I. A.-D. a. P. Choe, "A Framework of Information Security Integrated with Human Factors," *HCI for Cybersecurity, Privacy, Trust*, pp. 217-229, 2019.
- [12] B. Naqvi, "Mitigation strategies against the phishing attacks: A systematic literature review," *Computers & Security*, vol. 132, no. 1, pp. 1-25, 2023.
- [13] S. G.-Z. a. R. D. Gustavo González-Granadillo, "Security Information and Event Management (SIEM): Analysis,Trends, and Usage in Critical Infrastructures," *Sensors*, vol. 21, no. 14, pp. 1-2, 2021.
- [14] NIST, "Guide to Intrusion Detection and Prevention Systems (IDPS)," NIST, Gaithersburg, 2007.
- [15] "An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors," *Journal of Cybersecurity and Privacy*, vol. 1, no. 3, p. 387, 2021.
- [16] I. Alsmadi, "Incident Response," *The NICE Cybersecurity framework*, pp. 332-343, 2023.
- [17] F. M. S. Simone Buseti, "Evaluating incident reporting in cybersecurity. From threat detection to policy learning," *Government Information Quarterly*, vol. 42, no. 1, pp. 1-2, 2025.
- [18] NIST, "Data classification concept and Considerations for Improving Data Protection," NIST, 2023.
- [19] A. B. I. Olajide Soji Osundare, "Advancing network security in fintech: Implementing IPSEC VPN and cisco firepower in financial systems," *Science and technology*, pp. 27-29, 2024.