

Synthesize a Solution to a Potential Real-life Scenario

WORD COUNT: 1,996

ACCA4024: NETWORK & CYBERSECURITY FUNDAMENTALS
JOE FROHWEIN | 2315545

UNIVERSITY OF WALES TRINITY SAINT DAVID

SYNTHESIZE A SOLUTION TO A POTENTIAL REAL-LIFE SCENARIO

Joe Frohwein

Student University of Wales Trinity St David, Swansea, Wales

2315545@student.uwtsd.ac.uk

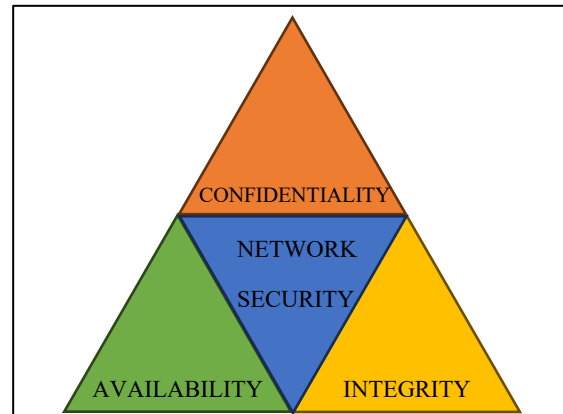
Abstract- This report outlines the new proposed comprehensive network security policy for a medium-sized financial services company, FinSecure Ltd, who deal with the sensitive data of their customers. This new security policy is essential to mitigate against threats that could compromise the confidentiality, integrity and availability of the company's network. This security policy implements industry standard policies and guidelines, mitigation measures, network monitoring & incident response, and a staff training program.

I. Introduction

As a medium-sized financial services company, FinSecure Ltd must ensure that a high level of network security is required. Network Security “refers to the technologies, policies, people, and procedures that defend any communication infrastructure from cyberattacks, unauthorized access, and data loss” [1].

The main purpose of network security is to protect and safeguard against threats. A threat is anything that may violate the CIA triad. The CIA triad is detailed below:

- Confidentiality – “Ensuring that sensitive data is accessed only by authorized individuals or systems”
- Integrity – “Ensuring data remains accurate, consistent, and unaltered during transmission or storage”
- Availability – “Ensuring data and network resources are accessible to authorized users when needed” [2]



(Figure 1 – The CIA triad)

Failure to meet each area of the CIA triad and therefore failing to achieve a high level of network security, our company will be vulnerable to a wide range of threats that will be covered in part A of the body section of this report.

As FinSecure Ltd is a financial services company, a lot of it's work can be performed remotely, with staff accessing the company's network from various locations using personal devices, which increases the company's vulnerability to threats, which adds greater importance to the protection of the company's data, devices and resources.

This lack of security could negatively impact the company, in ways such as:

- A decrease in productivity
- Loss of revenue
- Loss of sensitive data
- Loss of reputation & customer trust
- Loss of time & communications

- Threat to safety systems

Therefore, the company must implement a security policy so that it can avoid all these negative impacts to our company.

“Security policies govern the integrity and safety of the network. They provide rules for accessing the network, connecting to the Internet, adding or modifying devices or services, and more” [3].

The purpose of this report is to outline the objective and details of developing a new comprehensive security policy for FinSecure Ltd, demonstrating the need to mitigate both internal and external threats, in order to protect the company’s online resources.

II. Body

A. Identification of Threats

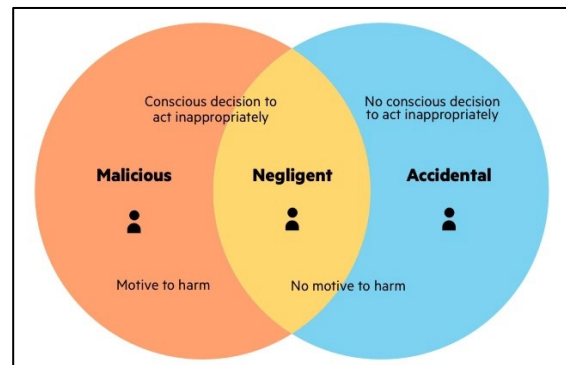
This section of the report will refer to threat and vulnerabilities. A threat is “a potential for a threat agent to exploit a vulnerability” and a vulnerability is “a flaw or weakness in an asset’s design, implementation, or operation and management that could be exploited by a threat” [4].

Threats can be both internal, meaning from inside of the company, or external, meaning from outside of the company.

Internal threats can arise from maliciousness or negligence, as well as being purely accidental, meaning a threat could both intentional or unintentional while possibly stemming from either proper or improper conduct. Potential internal threats to FinSecure Ltd could be:

- Insider attacks from current or ex-employees, who could damage systems or release sensitive information.

- Poor password management, compromising the security of the company.
- Weak access controls and unauthorised privileges, allowing unauthorised users to access sensitive data and systems.
- Negligent behaviour, allowing users to perform risky actions, which could be prevented with robust security protocols.



(Figure 2 – The difference between malicious, negligent and accidental behaviour [5])

External threats are typically only malicious, stemming from cybercriminals who are attempting to gain access to a company’s sensitive data or systems. Potential external threats could be:

- Phishing attacks, which is a modern form of social engineering where an attacker poses as an external entity, sending fraudulent messages encouraging users to sharing sensitive data or login credentials.
- Malware attacks, which is a type of software designed to cause harm to a company’s systems in the form of viruses/trojans.

- Ransomware attacks, which is a more modern trend of malware where the cybercriminal will demand a payment to remove the harmful software from your system.
- Distributed Denial-of-Service (DDoS) attacks, which is done by flooding a company's network with traffic, making it inaccessible for any other users. [6]

B. Security Policies

As stated in the introduction, a security policy is a course of action which is used by a company to govern a network and provide a set of rules, guidelines and requirements to be followed by all users.

A security policy will be created in accordance with industry security standards, which are documents written by subject experts that outline the best practices for that industry, with the CIA triad as a main priority throughout. The main standards that I believe FinSecure's security policy should be based on are:

- ISO/IEC 27001

An international standard for Information Security management. Complying with this standard will lead to greater security, advanced strategies and continuous improvement throughout the company [7].

- NIST Cybersecurity Framework (CSF)

A framework developed by the National Institute of Standards and Technology (NIST) which helps to improve the cybersecurity of a company's critical infrastructure by providing guidance to

organisations on how to manage their cybersecurity risks [8].

In accordance with these standards, the policies that I believe should be implemented within FinSecure Ltd are:

- Acceptable Use Policy (AUP)

Defines what is considered as acceptable and proper usage of a company's information, systems and resources. This improves data confidentiality by preventing improper use of sensitive data.

- Data Protection and Privacy Policy

Defines the compliance of a company with data protection regulations, such as the GDPR, whilst also defining how sensitive data should be collected, processed and stored. This improves data integrity by ensuring that data is accurate and unaltered.

- Data Access Control Policy

Defines the classification of data based on its type and sensitivity, and the authorisation of users to the data based on their role/authority. This improves data availability by ensuring users can access data which they're authorised to, without downtime or waiting for authorisation.

- Remote Access Policy

Defines how an employee is allowed to connect to and use a company's IT system. This policy is particularly important because of, as previously stated, the increased amount of remote working and staff accessing the IT systems from various locations and devices. This improves each area of the CIA triad by ensuring remote connections are secure, protected and readily available.

C. Mitigation Measures

Alongside these policies, to adequately reduce the company's vulnerability to threats, a series of mitigation measures must be implemented. A mitigation measure refers to "processes and technologies to reduce cybersecurity risks in an organisation's IT environment" [9].

The main mitigation measures that must be implemented, to improve the quality of the CIA triad criteria, are:

- Symmetric encryption

A form of encryption where the same pre-shared encryption key is used to encrypt and decrypt data. This form of encryption allows for faster data encryption and decryption due to lower CPU when compared to asymmetric encryption [10].

- Data Masking

A method of data transmission where sensitive data is replaced with a non-sensitive version, which is achieved by substituting, shuffling or nulling out the original data, in order to protect it from risky users/behaviour [11].

- Steganography

A form of data transmission where sensitive data is stored in the form of a graphic, audio or video file, in order to send it inconspicuously to repel attention from interceptors [12].

- Salting

A form of encryption where sensitive information, such as a password, is passed into a 'hash function' which converts it into an encrypted 'hash value'. Salting differs from hashing by ensuring that every outputted hashed

character string will be unique, even if the input was identical. To implement this, a cryptographically secure pseudo-random number generator (CSPRNG) would be used to generate the random character string to ensure that its unique, never reused, of the correct length and always in hash form when being transmitted [13].

D. Monitoring and Response

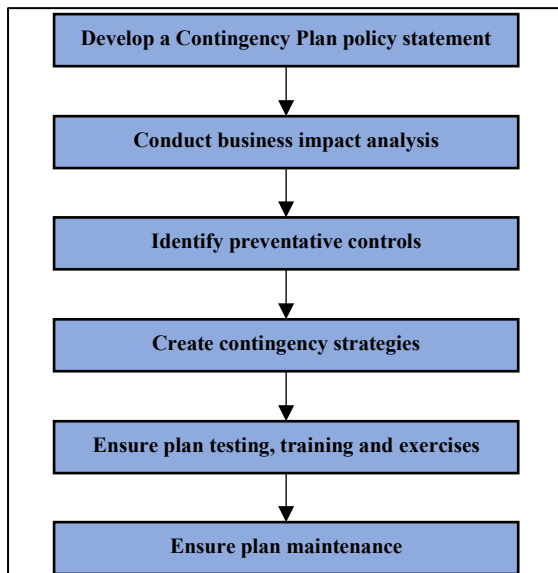
Whilst implementing this new security policy, the company must continue to monitor and respond to any security threats that may not have been prevented by the security policies and mitigation measures. Having a proactive incident response plan in place will help the company to react quickly to reduce negative effects.

This plan will involve the following steps:

- Develop a contingency plan policy statement, outlining the need for a contingency plan.
- Conduct business impact analysis, identifying the adverse effects that could impact the company's operations.
- Identify preventative controls by performing risk assessments and evaluating & implementing potential controls.
- Create contingency strategies, outlining the plan of action in the instance of a threat occurring
- Develop a contingency plan, which is the documentation of all previous steps, so all information, procedures and outcomes are clearly stated.
- Ensure plan testing, training and exercises, preparing all employees

and personnel to carry out the documented steps, which could be done through a series of drills, simulations and courses.

- Ensure plan maintenance, in order to keep the plan relevant, up to date and effective.



(Figure 3 – A flowchart outlining the plan for monitoring the network and responding to security incidents)

E. Training and Awareness

All users of a network will have some form of responsibility in ensuring that confidentiality, integrity and availability is implemented throughout. A structured cybersecurity training program is essential to ensure that all staff at FinSecure Ltd must be trained adequately to ensure that all sensitive data is kept secure, whilst also improving staff competency to reduce the risk of cyber threat due to negligence, human error or improper use.

Implementing this training plan will reduce the risk of data breaches and financial losses, as well as improving our data security standard compliance.

As previously mentioned, there are several modern trends of cyber threats, such as ransomware and social engineering tactics that all staff must be made aware of and trained regularly to ensure that their ability to avoid these modern threats is always up to date and relevant.

This training could be provided through methods such as:

- Presentations or lectures from industry experts, who can give staff a foundational base of knowledge related to explain and demonstrate the severity and risk of cybersecurity threats, and to share their experiences with new modern trends in cybercriminal activity, such as ransomware and social engineering tactics.
- Initial training and e-learning modules based on the new cybersecurity policy, in order to inform staff of the changes and how they will work and be implemented etc.
- Regular refresher courses, which could include quizzes, assessments and presentations/videos, to keep staff up to date and informed of any new updates to the security policy.
- Random simulated attacks, including phishing and social engineering simulations, in order to maintain staff awareness, cautiousness and vigilance to the increasing risk of security threats.
- Remote work training, to ensure that the staff that choose to work remotely are informed on the best remote work practices, such as using a VPN or connecting to public wi-fi sources.

III. Conclusion

To conclude, as a financial services company with large amounts of sensitive data, as well as a large amount of remote work staff, FinSecure Ltd must ensure a high level of cyber security. The increasing risk of both internal and external cyber threats highlights the need for the to improve the company's standards of the CIA triad. This can be achieved by implementing a new comprehensive security policy throughout the company.

This security policy will involve implementing several rules, requirements and policies, written in accordance with industry standards, which will establish clear defined guidelines to protect the company's resources and data.

These guidelines will be further strengthened by implementing a series of mitigation measures, which will be

updated regularly, in order to continuously improve the company's defence against modern cyberattacks.

These policies and mitigation measures will be regularly assessed by the 'Monitoring and Response' plan which will be implemented, allowing for fast response to threats.

Staff will be trained, in accordance with the new 'Training and Awareness' plan, which will be essential to establish a culture of cybersecurity awareness throughout the company.

By implementing each point of this security policy, FinSecure Ltd can increase its resilience to cyber threats, significantly improving the safety of its resources and sensitive customer data, leading to a greater trust from new and existing customers, which will lead to an increase in the company's sales revenue.

References

- [1] “Definition: What Is Network Security?,” Fortinet, [Online]. Available: <https://www.fortinet.com/resources/cyberglossary/what-is-network-security#:~:text=Network%20security%20refers%20to%20the%20technologies%2C%20policies%2C%20people%2C,infrastructure%20from%20cyberattacks%2C%20unauthorized%20access%2C%20and%20data%20loss..> [Accessed 18 03 2025].
- [2] C. W. Team, “What is the CIA Triad (Confidentiality, Integrity, Availability)?,” Cyber Security News, 13 11 2024. [Online]. Available: <https://cybersecuritynews.com/cia-triad-confidentiality-integrity-availability/>. [Accessed 18 03 2025].
- [3] “What Is Network Security Policy Management?,” Cisco, [Online]. Available: <https://www.cisco.com/site/us/en/learn/topics/security/what-is-network-security-policy-management.html>. [Accessed 18 03 2025].
- [4] L. Brow and W. Stallings, Computer Security: Principles and Practice, Pearson, 2023.
- [5] “Insider Threat,” imperva, [Online]. Available: <https://www.imperva.com/learn/application-security/insider-threats/>. [Accessed 21 03 2025].
- [6] “Cybersecurity Unveiled: Understanding External and Internal Threats,” With Secure, 24 04 2024. [Online]. Available: <https://www.withsecure.com/en/expertise/blog-posts/external-and-internal-threats>. [Accessed 21 03 2025].
- [7] “ISO/IEC 27001 – Information Security,” imsm, [Online]. Available: <https://www.imsm.com/ie/iso-27001/>. [Accessed 21 03 2025].
- [8] “The NIST Cybersecurity framework,” NIST, 24 02 2024. [Online]. Available: <https://www.nist.gov/cyberframework>. [Accessed 21 03 2025].
- [9] “What is cyber risk mitigation?,” Data Guard, 26 09 2024. [Online]. Available: <https://www.dataguard.com/blog/cyber-risk-mitigation-strategies/#:~:text=Common%20Cyber%20Risk%20Mitigation%20Strategies,and%20cybersecurity%20training%20for%20employees..> [Accessed 21 03 2025].
- [10] A. Badman and M. Kosinski, “What is symmetric encryption?,” IBM, [Online]. Available: <https://www.ibm.com/think/topics/symmetric-encryption#:~:text=Symmetric%20encryption%20is%20an%20encryption,it%20requires%20less%20processing%20power..> [Accessed 21 03 2025].
- [11] “Data Masking,” imperva, [Online]. Available: <https://www.imperva.com/learn/data-security/data-masking/>. [Accessed 21 03 2025].

- [12] “What is steganography? Definition and explanation,” kaspersky, [Online]. Available: <https://www.kaspersky.com/resource-center/definitions/what-is-steganography>. [Accessed 21 03 2025].
- [13] F. O'Sullivan, “What is password hashing and salting?,” Proton, 07 06 2024. [Online]. Available: <https://proton.me/blog/password-hashing-salting#salting>. [Accessed 21 03 2025].

Appendices

Proposed new Security Policy for FinSecure Ltd

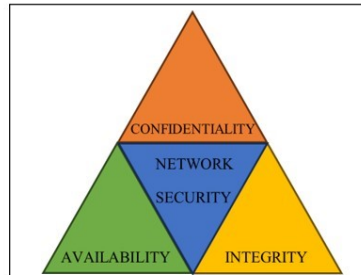
Joe Frohwein | 2315545

Background Information - Threats, Vulnerabilities and Security

- ▶ Network security “refers to the technologies, policies, people, and procedures that defend any communication infrastructure from cyberattacks, unauthorized access, and data loss”.
- ▶ Network Security is not about the removal of risk but is about the management of risk.
- ▶ Risk is the potential loss that the company could experience as a result of the balance of threat, vulnerabilities, countermeasures and values.
- ▶ A threat is “a potential for a threat agent to exploit a vulnerability”.
- ▶ A vulnerability is “a flaw or weakness in an asset’s design, implementation, or operation and management that could be exploited by a threat”.

Background Information - The CIA triad

- ▶ The purpose of network security is to protect against threats.
- ▶ Threats can be safeguarded against by ensuring that our network achieves each point of the CIA triad.
- ▶ **C**onfidentiality - “Ensuring that sensitive data is accessed only by authorized individuals or systems”
- ▶ **I**ntegrity - “Ensuring data remains accurate, consistent, and unaltered during transmission or storage”
- ▶ **A**vailability - “Ensuring data and network resources are accessible to authorized users when needed”



Our business and its need for a security policy - Sensitive data

- ▶ We are a medium-sized financial services company, who deal with a large amount of sensitive data from our customers, such as banking details, financial information and personal customer information.
- ▶ As a business, we must ensure a high level of network security in order to protect the security of our network.

Our business and its need for a security policy - Remote work

- ▶ As a financial services company, not much of our work tends to be physical.
- ▶ This gives us the opportunity to work and access the network remotely.
- ▶ Remote working has several advantages, but also some disadvantages.
- ▶ One main disadvantage of remote working is that staff will be accessing the network from a range of locations and personal devices.
- ▶ These remote connections will increase the network's vulnerability to threat

Our business and its need for a security policy - Potential Negative Effects

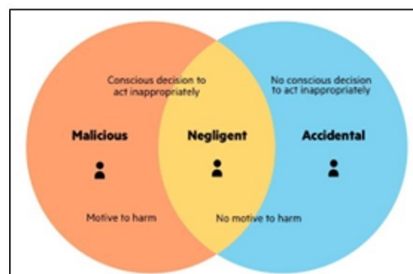
- ▶ If, as a company, we continue to act without adequate levels of cybersecurity being implemented, we could be negatively impacted in several ways, such as:
 - A decrease in productivity
 - Loss of revenue
 - Loss of sensitive data
 - Loss of reputation & customer trust
 - Loss of time & communications
 - Threat to safety systems

Our business and its need for a security policy - Security Policy

- ▶ To avoid the possibility of these potential negative effects impacting our company, we must implement a security policy.
- ▶ “Security policies govern the integrity and safety of the network. They provide rules for accessing the network, connecting to the Internet, adding or modifying devices or services, and more”.
- ▶ The development of this new comprehensive security policy is documented on the following slides.

Security Policy - Identification of Threats

- ▶ As mentioned previously, a threat is “a potential for a threat agent to exploit a vulnerability”.
- ▶ Threats to our company can come from both internal and external sources, meaning to come from inside or outside of the business.
- ▶ Threats can also arise from malicious, negligent, or accidental behaviour.
- ▶ Malicious users tend to be cybercriminals, whereas accidental and negligent users tend to be staff who cause threat through human error and improper use, respectively.



Security Policy - Identification of Threats (Internal)

Threat	Explanation
Insider attacks	Current or ex-employees who could intentionally damage systems or release sensitive information to third parties.
Poor password management	Ineffective passwords allowing login credentials to be accessed by unauthorised users.
Weak access controls and unauthorised privileges	Unauthorised users could gain access to systems or data which they should not be authorised to.
Negligent behaviour	Users who perform risky behaviour and actions, either due to lack of training or a lack of care for the company

Security Policy - Identification of Threats (External)

Threat	Explanation
Phishing attacks	A modern form of social engineering where an attacker poses as an external entity, sending fraudulent messages encouraging users to sharing sensitive data or login credentials.
Malware attacks	A virus software that is designed to cause harm to a company's resources.
Ransomware attacks	A more modern trend version of malware, where a cybercriminal demands a payment to reverse the effects of the malware.
Distributed Denial-of-Service (DDoS) attacks	A computer system is flooded with network traffic to cause downtime.

Security Policy - Industry Standards & Policies

- ▶ As previously stated, a security policy is a course of action which is used by a company to govern a network and provide a set of rules, guidelines and requirements to be followed by all users.
- ▶ A security policy will be created in accordance with industry security standards, which are documents written by subject experts that outline the best practices for that industry, with the CIA triad as a main priority throughout.

Security Policy - Industry Standards & Policies (Standards)

Industry Standard	Explanation
ISO/IEC 27001	An international standard for Information Security man management. Complying with this standard will lead to greater security, advanced strategies and continuous improvement throughout the company
NIST Cybersecurity Framework (CSF)	A framework developed by the National Institute of Standards and Technology (NIST) which helps to improve the cybersecurity of a company's critical infrastructure by providing guidance to organisations on how to manage their cybersecurity risks

Security Policy - Industry Standards & Policies (Policies)

Security Policy	Explanation
Acceptable Use Policy (AUP)	Defines what is considered as acceptable and proper usage of a company's resources.
Data Protection and Privacy Policy	Defines the compliance of a company with data protection regulations as well as defining how sensitive data should be collected, processed and stored.
Data Access Control Policy	Defines the classification of data based on its type and sensitivity, and the authorisation of users to the data based on their role/authority.
Remote Access Policy	Defines how an employee is allowed to connect to and use a company's IT system.

Security Policy - Mitigation Measures

- ▶ A mitigation measure refers to “processes and technologies to reduce cybersecurity risks in an organisation's IT environment”.
- ▶ Mitigation measures are essential to a robust cybersecurity policy as they act as an extra line of defence between threats and the network.
- ▶ A system of well implemented mitigation measures will reduce the company's vulnerability to threats.

Security Policy - Mitigation Measures (Examples)

Mitigation measure	Explanation
Symmetric encryption	Encryption with a pre-shared encryption key that is used encrypt and decrypt data.
Data masking	Sensitive data is replaced with a substituted, shuffled or nulled-out non-sensitive version of the data.
Steganography	Sensitive data is stored in the form of a graphic, audio file or video.
Salting	Encryption with sensitive information being stored as a randomly generated unique "hashed" character string.

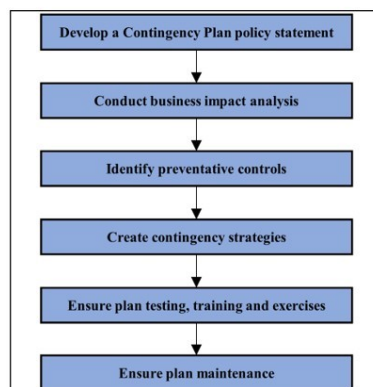
Security Policy - Monitoring & Response

- ▶ As this new Security Policy is developed and implemented, we must ensure that we continue to monitor and respond to any security threats that may have flown under the radar and bypassed the previously mentioned policies and mitigation measures.
- ▶ Having a proactive incident response plan in place will help the company to react quickly to reduce negative effects.

Security Policy - Monitoring & Response (Plan)

Step	Explanation
Develop a contingency plan policy statement	Outlines the need for a contingency plan.
Conduct business impact analysis	Identifies the adverse effects that could impact the company.
Identify preventative controls	Done through risk assessments and evaluating & implementing controls.
Create contingency strategies	Outlines the plan of action in the event of an occurred threat.
Develop a contingency plan	The documentation of all procedures and outcomes of a threat occurring.
Ensure plan testing and training	Prepares personnel for the possibility of a threat occurring.
Ensure plan maintenance	Keeps the plan relevant and up to date.

Security Policy - Monitoring & Response (Flow chart)



Security Policy - Training & Awareness

- ▶ Every user of a network has their own responsibilities to maintain the security of a network, performing different roles to do so, based on their role in the company.

Confidentiality	Integrity	Availability
User	User	IT administrator
IT administrator	IT administrator	Network administrator
Network administrator	Network administrator	Third-party vendor
HR	HR	
Senior management	Senior management	

- ▶ Therefore, a structured cybersecurity training program is essential to implement, to ensure that all staff are adequately trained, to ensure competency and awareness of the new security policy.

Security Policy - Training & Awareness (Requirement)

- ▶ We must ensure that the staff training is implemented and delivered so that staff are competent, therefore reducing the risk of cyber threat due to negligence, human error or improper use.
- ▶ In addition, due to the increasing level of cybersecurity threats and the ever-changing modern trends in cybercriminal activity, we must ensure that all staff are well aware and regularly updated and trained to maintain their vigilance to these threats.

Security Policy - Training & Awareness (Plan)

Training method	Explanation
Presentation from industry experts	Can give relevant case studies and experiences of cybersecurity threats and how to reduce their risk, improving the staff's awareness.
Initial training courses	Informs staff of the new security policy and how they must now act in accordance with it.
Regular refresher training courses	Keeps staff up to date and informed of any new updates to the security policy.
Random simulated cyber attacks	Maintain staff awareness, cautiousness and vigilance to cyber threats.
Remote work training courses	Informs staff of best practices and behaviour when working remotely.

Conclusion

- ▶ As a financial services company with large amounts of sensitive data, as well as a large amount of remote work staff, FinSecure Ltd must ensure a high level of cyber security, so that we can continue to maintain a high level of confidentiality, integrity and availability throughout our business.
- ▶ A new security policy has been developed and will be implemented, so that we can increase our resilience to cyber threats, significantly improving the safety of our resources and sensitive customer data, leading to a greater trust from new and existing customers, which will lead to an increase revenue.
- ▶ The security policy will contain:
 - Security Standards and Policies
 - Mitigation Measures
 - Monitoring & Response
 - Training & Awareness