

12/19/2025

Synthesize a Solution to a potential Real-life Scenario

Network and Cyber Security Essentials



Student Name: Jasin Navas

Student ID: 2426726

Programme: CertHE Computing Skills for Workplace

Module Code: ACCA4024

Module Name: Network and Cyber Security

Lecturer's Name: Dr Kwame Assa-Agyei

Table of Contents

Cybersecurity Policy Development for Revolute	2
Abstract.....	2
Introduction.....	2
Identification of Modern Threats	3
Modern Security Policies.....	4
Technical Mitigation Measures.....	5
Proactive Monitoring and Incident Response	5
Continuous Training and Awareness	8
Conclusion	8
References.....	10
Appendix A: Screenshot of the Board of Directors PowerPoint presentation	11
Appendix B: Screenshot of the Badge	15

Cybersecurity Policy Development for Revolute

Abstract

Cybersecurity is a serious global issue because cyberattacks are becoming more advanced and more frequent. Remote and hybrid working, along with greater use of cloud services, have increased security risks. Fintech companies like Revolut are common targets because they handle sensitive financial information.

This report describes a simple Zero Trust security approach to help protect against modern cyber threats. It focuses on risks such as ransomware attacks, AI-based scam calls, supply chain attacks, and cloud security problems. The report explains how strong security controls, continuous monitoring, and regular employee training can improve overall protection.

Here, some Diagrams are used to show how Zero Trust security and monitoring systems work, helping to explain how organisations can stay secure in a changing cyber threat environment

Introduction

Revolut is a fintech company based in the UK that offers millions of users worldwide online banking, payment, and cryptocurrency services. The company can expand quickly and provide services to clients with ease because it primarily uses cloud systems and mobile apps. However, the risk of cyberattacks is also increased by this method of operation.

These days, many employees work remotely or in hybrid roles, and the business makes extensive use of mobile devices and online software. Attackers can more easily identify vulnerabilities like compromised software, phony emails, or stolen passwords as a result. The seriousness of these risks is demonstrated by recent cyber incidents in the financial sector, such as ransomware attacks and phishing scams.

To deal with these threats, For Revolut I decided to use a Zero Trust security approach. This means that no user or device is trusted automatically, even if they are inside the company network. Everyone must prove who they are, and access is limited to only what is necessary. This approach uses clear security rules, strong technical protections, constant monitoring for suspicious activity, and regular staff training.

This report explains how Revolut can improve its security by first identifying risks, then protecting systems, detecting attacks early, responding quickly when incidents happen, and finally recovering systems safely. It also explains how these steps help keep customer data private, accurate, and always available for use.

Identification of Modern Threats

Ransomware-as-a-Service (RaaS): Ransomware-as-a-Service (RaaS) is a cybercrime business model where developers offer ready-built ransomware kits via darknet markets to affiliates who launch attacks without needing to build malware from scratch. This lowers technical barriers and increases the frequency and scale of attacks against corporate networks [1].

Criminal groups offer ransomware kits to affiliates, lowering barriers to entry. Ransomware-as-a-Service (RaaS) is a model where hackers sell or rent ready-made ransomware tools to others. Less-skilled criminals can use these tools to launch attacks, sharing any ransom with the creators.

RaaS is dangerous for companies like Revolut because it makes attacks easier and more frequent. Since Revolut handles sensitive financial data, even short disruptions could cause financial losses, reputational damage, and loss of customer trust [1].

AI-powered vishing/social engineering: With advances in artificial intelligence, attackers can now create very realistic fake voices and fake identities. This makes it easier for them to trick people over the phone. Revolut's customer support teams are at risk from these AI-driven "vishing" attacks, where attackers pretend to be someone trustworthy to steal personal or financial information. These attacks rely on human trust, making them hard to detect and potentially very harmful [2].

Supply Chain Compromises: Instead of attacking a Company directly, hackers often target **third-party vendors or software providers** that Revolut depends on. If these external partners are compromised, attackers can use them as a gateway into Revolut's systems. This type of attack is known as a **supply chain attack** [3].

The **MOVEit** breach is a clear example of how a vulnerability in a widely used **Managed File Transfer (MFT)** tool allowed attackers to compromise many organizations at the same time.

Since Revolut relies heavily on **Application Programming Interfaces (APIs)** and **Software as a Service (SaaS) platform**, any security weakness in these external systems can significantly increase its overall cybersecurity risk [4]

Cloud Misconfigurations: It will happen when cloud services such as **Amazon Web Services (AWS)** or **Google Cloud Platform (GCP)** are set up with **wrong or insecure settings**. These mistakes can include leaving **storage buckets open to the public**, having **weak access controls**, or not using **encryption** to protect data in storage or during transfer. Because Revolut uses cloud-native systems, it must manage these settings carefully, so sensitive information is not leaked, and compliance rules are not broken [1].

Modern Security Policies

Revolut is advised to follow **Zero Trust security principles** and international cybersecurity standards, meaning that no user or system is automatically trusted.

- **Identity and Access Management (IAM):** Company should enforce strong **Identity and Access Management** controls by implementing **Multi-Factor Authentication (MFA)** and **conditional access policies** across all systems. Adopting **password less authentication** methods will further reduce the risk of credential theft and account compromise [5].
- **Least Privilege Access:** Apply the **principle of least privilege** using **Role-Based Access Control (RBAC)** and **micro-segmentation** to restrict access and limit lateral movement during a security breach.
- **Data Security:** Classify customer data based on sensitivity and protect it using **encryption** at rest and in transit. Implement **Data Loss Prevention (DLP)** policies to prevent unauthorised data sharing and support regulatory compliance.
- **Cloud and SaaS Security:** Use **Cloud Security Posture Management (CSPM)** tools to continuously monitor cloud configurations. Deploy **Cloud Access Security Broker (CASB)** solutions to control access to **Software as a Service (SaaS)** application.
- **Vendor Risk Management:** Continuously assess **third-party vendor risks** and enforce security requirements through contractual agreements to reduce supply chain threats.

- **Incident Response Policy:** Follow **NIST Special Publication 800-61** to ensure clear incident detection, escalation paths, and communication procedures during cybersecurity incidents [6].

Technical Mitigation Measures

To mitigate key cybersecurity threats, it is recommended that Revolut deploys layered technical security controls based on Zero Trust principles.

- **Identity Security:** Strengthen user authentication by using **Multi-Factor Authentication (MFA)**, **Privileged Access Management (PAM)**, and adaptive login methods to lower the risk of unauthorised access [5].
- **Endpoint Security:** Protect computers and mobile devices by deploying **Endpoint Detection and Response (EDR)** or **Extended Detection and Response (XDR)** tools, supported by **Mobile Device Management (MDM)**.
- **Network Security:** Limit network access by using **Zero Trust Network Access (ZTNA)** and **micro-segmentation**, which help prevent attackers from moving across systems if a breach occurs [5].
- **Cloud Security:** Secure cloud data through **Encryption** during storage and transfer and maintain immutable backups to improve protection against ransomware attacks.
- **Security Monitoring:** Use a **Security Information and Event Management (SIEM)** system combined with threat intelligence feeds to better detect and respond to security threats.
- **Patch Management:** Fix security weaknesses based on priority by following the **CISA Known Exploited Vulnerabilities (KEV) Catalogue**, focusing first on vulnerabilities that are actively being exploited [6].

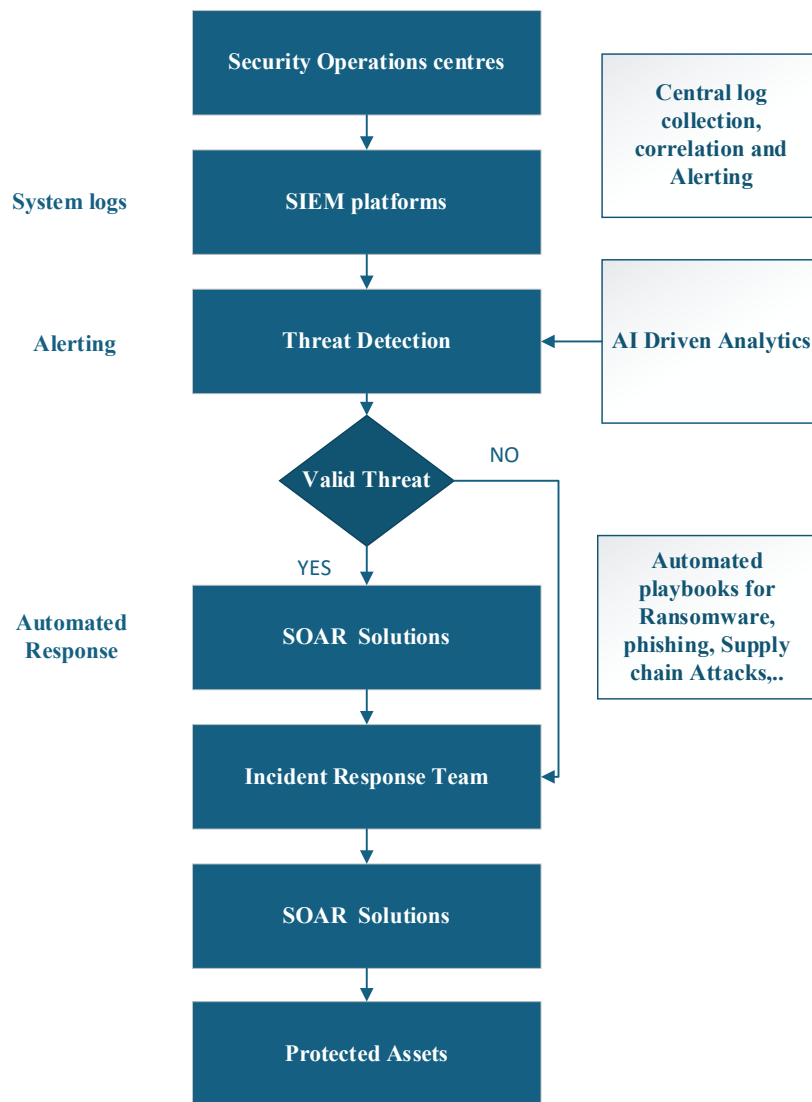
Proactive Monitoring and Incident Response

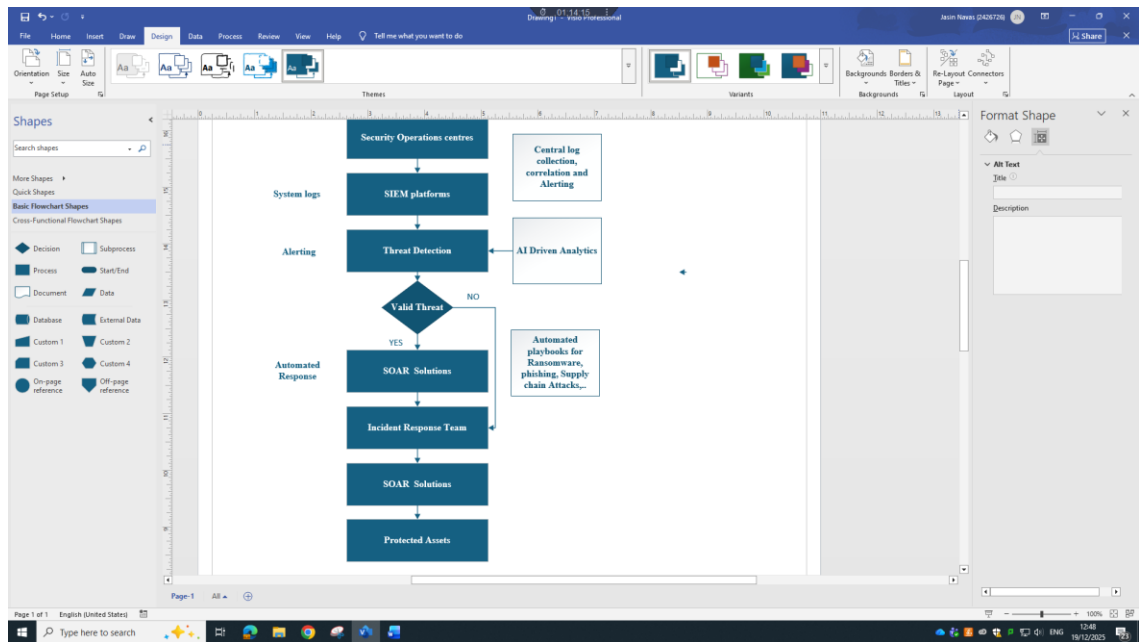
To effectively detect and respond to cyber threats, it is recommended that **Revolut's Security Operations Centre (SOC)** operates on a **24/7 basis**, supported by advanced monitoring tools and automated response capabilities [6].

A **Security Information and Event Management (SIEM)** platform should be used to centrally collect, correlate, and analyse system logs, enabling timely alerting and improved

threat visibility. In addition, **Security Orchestration, Automation, and Response (SOAR)** solutions should be implemented to automate response playbooks for common incidents such as ransomware, phishing, and supply chain attacks, reducing response time and human error [6].

Furthermore, **AI-driven behavioural analytics** should be adopted to identify unusual activities and anomalies that may not be detected by traditional rule-based security controls, improving early threat detection and incident response effectiveness [7].





Continuous Training and Awareness

As human error is a major cause of cybersecurity incidents, it is recommended that **Revolut establishes a strong organisational culture of security awareness**. Regular **phishing and vishing simulations** should be conducted to improve employees' ability to recognise social engineering attacks [6]. **Role-specific training** should be provided, such as secure coding practices for developers and vishing awareness for customer support staff, to address job-related security risks [6].

The use of **interactive and gamified learning tools** is encouraged to increase engagement and improve knowledge retention.

The effectiveness of training programmes should be measured by monitoring **phishing click rates** and **incident reporting levels** [6]. In addition, visible involvement from senior management is essential to reinforce the message that **cybersecurity is a shared responsibility across the organisation** [7].

Conclusion

By doing this assignment I taught a lot about why cybersecurity is so important for companies like Revolut. I learned that cyberattacks today are more advanced and happen more often, which means old security methods are not enough anymore.

One of the most important things I discovered is the **Zero Trust approach**. This method does not automatically trust anyone or any device, even if they are inside the company network. Instead, everyone must prove who they are before getting access, and they only get the minimum access they need. This makes it much harder for hackers to move around inside the system if they manage to break in.

I also learned that good security is not just about technology. It needs strong tools like **monitoring systems**, quick response plans, and regular **employee training** because human mistakes are one of the biggest reasons attacks succeed. Things like phishing emails or fake phone calls can trick people easily, so training is very important.

Another key point I learned is that security is an ongoing process. Companies must keep updating their systems, checking for weaknesses, and working with trusted vendors to avoid supply chain attacks. They also need to protect cloud services because wrong settings can lead to data leaks.

Overall, this assignment showed me that cybersecurity is about protecting customer data, following rules and regulations, and keeping customer trust. A strong security plan helps the company stay safe, avoid financial losses, and maintain its reputation.

References

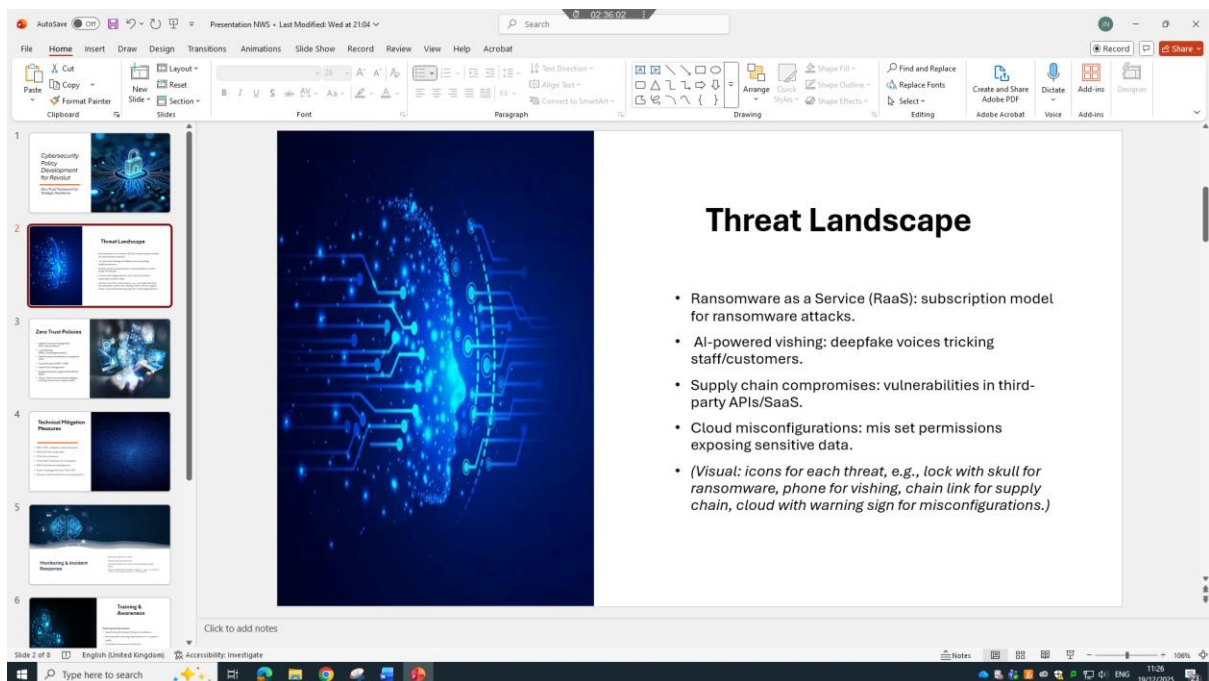
- [“Ransom ware as a Service (RaaS): Emerging Threats and Proactive Defense Tactics,” vol. 8, no.
1 10, 30-04-2025.
]
- [Andreas Triantafyllopoulos, Anika A. Spiesberger, Iosif Tsangko, Xin Jing, Verena Distler, Felix
2 Dietz, Florian Alt, Björn W. Schuller, “Vishing: Detecting social engineering in spoken
] communication”.
- [Betul Gokkaya, Leonardo Aniello, Basel Halak, “Software supply chain: review of attacks, risk
3 assessment strategies and security controls,” May 2023. [Online]. Available:
] https://www.researchgate.net/publication/370981353_Software_supply_chain_review_of_attacks_risk_assessment_strategies_and_security_controls.
- [U. k. A. B. G. khan, “ANALYSING THE EXPLOITATION OF MOVEIT AND MOVEIT
4 CLOUD: CYBERSECURITY RISKS, ATTACK VECTORS, AND MITIGATION
] STRATEGIES”.
- [J. Kindervag, “Build Security Into Your Network’s DNA: The Zero Trust Network,” November 11,
5 2010.
]
- [Alex Nelson, Sanjay Rekhi, Murugiah Souppaya, Karen Scarfone, “Incident Response
6 Recommendations,” [Online]. Available:
] <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf>.
- [“Security and Privacy Controls for Information Systems and Organizations,” National Institute of
7 Standards and Technology.
]

Appendix A: Screenshot of the Board of Directors PowerPoint presentation

Slide 1



Slide 2



Slide 3

The screenshot shows a PowerPoint presentation in Adobe Presenter. The slide is titled "Zero Trust Policies" and lists several key components of a Zero Trust architecture. The background features a hand holding a glowing digital interface with various icons representing security and connectivity.

Zero Trust Policies

- Identity & Access Management (MFA, passwordless).
- Least Privilege (RBAC, microsegmentation).
- Data Security (classification, encryption, DLP).
- Cloud Security (CSPM, CASB).
- Vendor Risk Management.
- Incident Response aligned with NIST SP 80061.
- *(Visual: Zero Trust architecture diagram showing "Never trust, always verify.")*

Slide 4

The screenshot shows a PowerPoint presentation in Adobe Presenter. The slide is titled "Technical Mitigation Measures" and lists several technical measures for implementing Zero Trust. The background features a dark blue circuit board pattern.

Technical Mitigation Measures

- MFA, PAM, adaptive authentication.
- EDR/XDR for endpoints.
- ZTNA for networks.
- Immutable backups & encryption.
- SIEM with threat intelligence.
- Patch management via CISA KEV.
- *(Visual: layered defence shield graphic.)*

Slide 5

AutoSave ON Presentation NWS - Last Modified Wed at 21:04

File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help Acrobat

1 Cybersecurity Policy Development for Resilient
2 Threat Landscape
3 Zero Trust Policies
4 Technical Mitigation Measures
5 **Monitoring & Incident Response**
6 Training & Awareness

Monitoring & Incident Response

- 24/7 SOC with SIEM + SOAR.
- AIdriven anomaly detection.
- Response playbooks: ransomware, phishing, supply chain.
- (Visual: SIEM/SOAR workflow diagram — logs → correlation → alert → automated response → escalation.)

Click to add notes

Slide 5 of 6 English (United Kingdom) Accessibility Investigate

Slide 6

AutoSave ON Presentation NWS - Last Modified Wed at 21:04

File Home Insert Draw Design Transitions Animations Slide Show Record Review View Help Acrobat

3 Zero Trust Policies
4 Technical Mitigation Measures
5 Monitoring & Incident Response
6 **Training & Awareness**
7 Business Impact
8 Conclusion

Training & Awareness

Training & Awareness

- Quarterly phishing/vishing simulations.
- Rolespecific training (developers vs. support staff).
- Gamified awareness modules.
- Metrics: reduced click rates, increased reporting.
- (Visual: cartoon of employees in training, phishing email simulation.)

Click to add notes

Slide 6 of 8 English (United Kingdom) Accessibility Investigate

Slide 7

The screenshot shows a PowerPoint presentation in edit mode. The slide is titled "Business Impact" and features a dark blue background with a world map and various icons representing business and technology. The slide content is as follows:

- Financial:** Avoid ransom payments, fines, fraud losses.
- Operational:** Prevent downtime, ensure service continuity.
- Reputational:** Maintain customer trust and regulatory compliance.
- (Visual: three pillars labeled Financial, Operational, Reputational.)*

The slide is part of a presentation titled "Presentation NWS - Last Modified: Wed at 21:04". The status bar at the bottom indicates "Slide 7 of 8" and "English (United Kingdom)".

Slide 8

The screenshot shows a PowerPoint presentation in edit mode. The slide is titled "Conclusion" and features a dark blue background with a wireframe figure wearing a VR headset and interacting with a network of icons. The slide content is as follows:

- Zero Trust = Strategic Investment in Resilience.
- Protects Revolut's customers, data, and brand.
- Aligns with FCA, GDPR, NIST CSF, ISO 27001.

The slide is part of a presentation titled "Presentation NWS - Last Modified: Wed at 21:04". The status bar at the bottom indicates "Slide 8 of 8" and "English (United Kingdom)".

Appendix B: Screenshot of the Badge

