Manchester Metropolitan University

Security Management Plan

HSBC (UK)

2024

Table of contents

Approval History

Version:	Reviewed By:	Approved By:	Approver's Position:	Date Approved:	Next Review Date:

Revision History

Version	Date	Author	Description

Glossary:

Abbreviations	
Abbreviation	**Expansion**
SMP	Security Management Plan

Abbreviations	
Abbreviation	**Expansion**

1 Introduction

1.1.1 Background

HSBC UK is a leading retail and commercial bank in the United Kingdom, serving millions of customers across the country.

HSBC is a multinational banking and financial services group, headquartered in London, the United Kingdom. It was set up on 3rd March 1865 in British Hong Kong, for helping finance trade between Europe and Asia by meeting global demands. Over more than 150 years, HSBC serve 62 countries and territories and almost 42 million personal, wealth, and business clients globally (HSBC, 2024). It offers a wide range of financial services, such as commercial banking, global banking and markets, private banking, retail banking, and wealth management; likewise aims to create new possibilities for clients by using their distinct knowledge, skills, range, and viewpoints (Trudeau and McLarney, 2017). In addition to helping finance trade between Europe and Asia, they bring together people, ideas, and resources that promote progress and growth (Trudeau and McLarney, 2017).

1.1.2 Data Privacy

HSBC UK is committed to complying to data privacy laws and regulations, including as the General Data Protection Regulation (GDPR) implementation since 2018 in the United Kingdom – Data Protection Act 2018 (Buckley, 2021). The Data Protection Act has been updated yearly since its implementation in 1998 and it guarantees privacy and legal use of personal data by businesses and organisations (Merhi, M. et al, 2019). Following these legal obligations is to ensure transparency, accountability, and individuals' rights over their personal information when the bank collects, utilises, and keeps customers' personal information.

1.1.3 Regulatory Compliance

HSBC UK is subject to regulations imposed by the Financial Conduct Authority (FCA) and other regulatory bodies. The FCA has emphasised that it will prioritize ensuring that financial services companies treat all their clients fairly, businesses may face enforcement action from the FCA if they fail to provide proper treatment to vulnerable customers (Powley and Stanton., 2020). HSBC UK must comply with FCA regulations, which include customer protection, market integrity, anti-money laundering measures, and other areas. In the Final Notice of FCA, published on 3rd October 2023, the FCA reiterated that regulated firms need adequate cyber security arrangements to protect the personal data they hold and that where data processing is outsourced, it must exercise

appropriate oversight over outsourced functions (FCA Final Notice, 2023). Additionally, the FCA can investigate and take enforcement action against firms that fail to comply with its rules and regulations (FCA Final Notice, 2023). This ensures for maintaining the stability and trustworthiness of the UK financial system.

1.1.4 Attacks in the industry

Financial institutions are the backbone of the economy and a vital component of crucial infrastructure. They are necessary for the proper operation of the global economy. However, financial institutions have recently faced an increase in cyber dangers. The attacks have increased in frequency, complexity, and destructiveness. The financial services sector, in particular, is a prime target for hackers.

Attack vectors include ransomware attacks, social engineering and phishing, as well as the growing quantity and intensity of cyber threats. Social engineering and phishing mainly target clients and staff, taking advantage of weaknesses made worse by the move to remote work brought on by the epidemic. Besides, ransomware attacks have increased, mainly targeting banks and other financial institutions globally. This underscores how more organisations need to understand security precautions. Despite ongoing efforts to educate, many consumers still inadvertently download malware through manipulated links or email attachments. Moreover, cyberattacks are no longer solely motivated by financial gain, but are increasingly aimed at disrupting networks and services. This evolving nature of cyber threats highlights the urgency for organisations and individuals to stay updated with the latest security measures. (Gulyás and Kiss, 2023)

Industry stakeholders must collaborate to share threat intelligence and best practices, reduce systematic risks, fortify the financial ecosystem's resilience, improve cybersecurity measures, raise user awareness, and allocate resources to proactive defence plans to counteract constantly evolving threats.

Cyber-attack to HSBC online banking (Guardian, 2016)

Reported on 29th Jan 2016, HSBC experienced a "denial-of-service" (DoS) attack that disrupted its internet banking services, leaving customers unable to access their accounts for several hours. However, the bank's proactive response was commendable. It defended its systems and assured that no transactions were affected, thereby mitigating the potential damage. While the inconvenience to customers was acknowledged, the bank's swift action was a testament to its commitment to customer security. Experts warn that denial-of-service attacks primarily aim to damage the

institution's reputation rather than directly target customer accounts. However, they can distract from more sinister activities like cyber-heists. HSBC learnt the importance of continually improving cybersecurity measures to protect against direct and indirect threats, ensuring the resilience of their online services, and maintaining customer trust.

Alleged Cyberattack and Banks Deny Breach to HSBC and Barclays (Ashish, 2024)

Allegations of a cyberattack on HSBC and Barclays banks have emerged, reportedly carried out by hackers IntelBroker and Sanggiero in April 2024. The breach allegedly facilitated through a third-party contractor, led to the leakage of sensitive data, including financial transactions and proprietary information. Despite the hackers' claims and data samples shared on Breachforums, both banks have denied any cybersecurity incident and refuted claims of data compromise. This incident serves as a stark reminder of the vulnerability of financial institutions to cyber threats, particularly through third-party relationships, and underscores the critical need for robust cybersecurity measures. The potential consequences including reputational damage to banks, financial losses, and potential legal repercussions, are all significant. In light of this, financial institutions must prioritize regular security assessments, strengthen vendor risk management protocols, and invest in comprehensive employee training to mitigate such risks and uphold trust with customers and stakeholders.

1.2 Purpose

This security management plan HSBC UK aims to provide a comprehensive overview of its security operating model, including the identification of information assets, assessment of threats and risks, selection of controls, and key implementation considerations. It serves as a guiding document to ensure alignment with organizational objectives, regulatory requirements, and industry best practices in maintaining the confidentiality, integrity, and availability of HSBC's information assets. Understanding the organization's scale and complexity is essential for understanding the security challenges it faces and the strategies outlined in the plan for mitigating related risks.

1.3 Readership

This Security Management Plan is intended for a diverse audience within HSBC UK, including but not limited to:

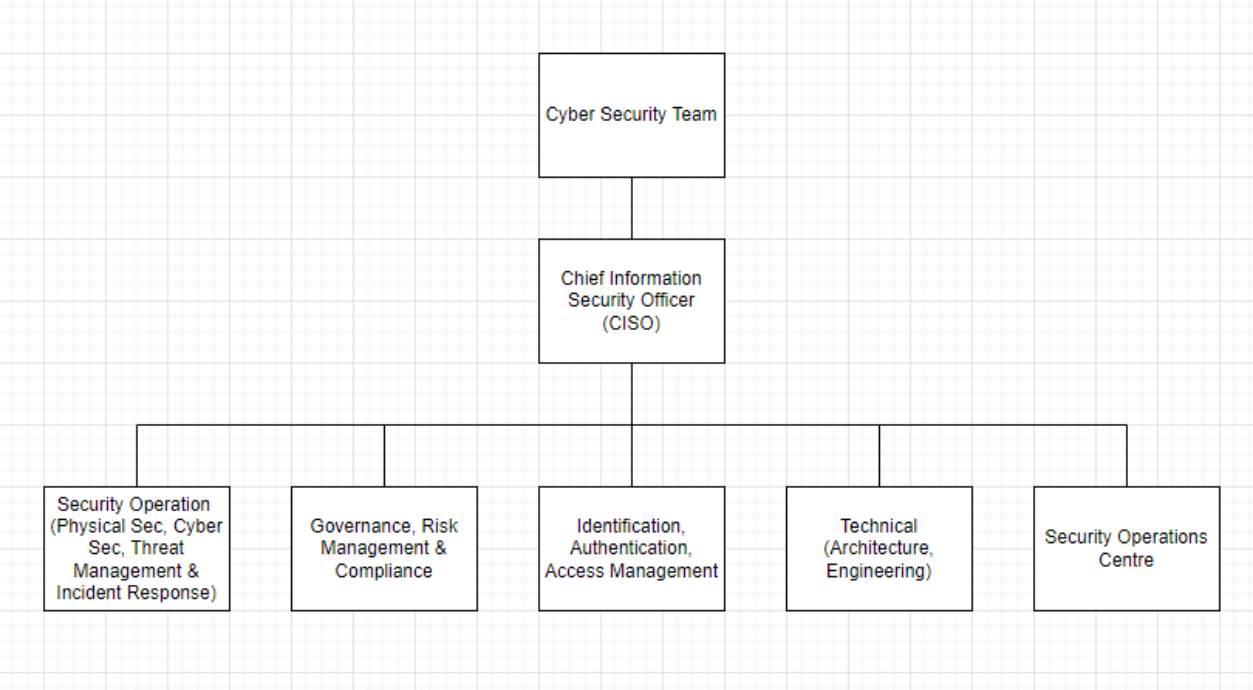
- Senior Management: Responsible for providing strategic direction and oversight of security initiatives, senior management will utilise this plan to align security objectives with organisational goals and allocate resources accordingly.
- Security Personnel: Security professionals tasked with implementing and enforcing security measures will refer to this plan for guidance on conducting risk assessments, developing security protocols, and responding to security incidents effectively.
- Internal Auditors: This role in maintaining a secure environment is vital. This Security Management Plan is a comprehensive reference tool that provides employees with knowledge and understanding of their responsibilities regarding security awareness, reporting procedures, and compliance with security policies.
- External Auditors: External partners and other stakeholders may also benefit from understanding HSBC UK's approach to security management. This plan provides transparency and reassurance regarding the organisation's commitment to protecting the interests of all stakeholders.

By addressing the needs of these critical stakeholders, HSBC UK aims to ensure widespread understanding and adherence to its specific security management objectives, such as prevent security breaches, ultimately strengthening its resilience against emerging threats.

2 Solution Operations Overview

2.1 Security control overview

As the Chief Information Security Officer (CISO) of HSBC UK, the Security Operating Model is designed to guarantee the safety of the company's digital assets and efficiently reduce cybersecurity threats. The model includes a number of groups and roles, all of which are essential to preserving the security posture of the business:



2.2 Security Operation Function

Chief Information Security Officer (CISO)

- Primarily responsible for establishing and maintaining the bank's information security strategy and policies; also responsible for safeguarding the confidentiality, integrity, and availability of the bank's information assets, including customer data and proprietary information.

Governance, Risk Management & Compliance (GRC):

Compliance Manager

- Develop, implement, and maintain compliance programs to ensure adherence to regulatory requirements and internal policies.
- Conduct compliance assessments, audits, and reviews to identify gaps and recommend corrective actions.

- Liaise with regulatory agencies and external auditors to facilitate compliance reviews and audits.
- Provide guidance and training to employees on compliance-related matters.
- Monitor regulatory changes and update compliance programs accordingly.

Risk Manager

- Identify, assess, and prioritize risks to HSBC UK's information assets, operations, and reputation. Develop risk management strategies and plans, a pivotal responsibility in mitigating identified risks within acceptable tolerance levels, thereby safeguarding HSBC UK's information assets, operations, and reputation.
- Conduct risk assessments using appropriate methodologies and tools, including risk identification, analysis, and evaluation.
- Monitor risk indicators and triggers and provide timely reporting and escalation of significant risks to senior management.
- Collaborate with business units to embed risk management practices into decision-making processes.

Policy & Standards Officer

- Develop, review, and maintain information security policies, standards, and procedures under industry best practices and regulatory requirements.
- Ensure that policies and standards are effectively communicated to all employees and relevant stakeholders.
- Monitor compliance with policies and standards and conduct periodic reviews and updates as necessary.
- Provide guidance and support to business units in interpreting and implementing security policies and standards.
- Collaborate with other teams to align security policies and standards with overall GRC objectives and initiatives.

Security Operations:

Physical Security Supervisor

- Responsible for security guards and closed-circuit television (CCTV) operators and ensure the effective implementation of access control, surveillance, and other

physical security protocols. To ensure the effective implementation of access control, surveillance, and other physical security protocols.

Cyber Security Analysts

- The team is responsible for threat intelligence; monitoring, analysing, and responding to cybersecurity threats and incidents, including maintaining network security and managing incident response procedures:
    - **Network Security Team**

      Manages and maintains the bank's network security infrastructure, including firewalls, intrusion detection systems, and network monitoring tools.
    - **Incident Response Management Team**

      Responds to and mitigates cybersecurity incidents, such as data breaches, malware infections, or unauthorised access attempts. They are responsible for containing incidents, conducting forensic analysis, and implementing remediation measures.

Identification, Authentication & Assessment Management:

Penetration Testing Team

- Responsible for simulating cyberattacks. Their comprehensive assessments, conducted using various techniques such as network scanning, web application testing, and social engineering, are instrumental in identifying potential security weaknesses. By emulating real-world attack scenarios, they pinpoint vulnerabilities that malicious actors could exploit. The team then provides detailed reports and recommendations to remediate these vulnerabilities, playing a crucial role in fortifying HSBC UK's defences and protecting against potential cyber threats.

Technical Team:

Architecture & Engineering

- To design and implement robust security measures across the IT infrastructure. This involves creating a layered defence strategy that encompasses network security, data protection, access control, and encryption mechanisms.
- A major component of the team's activity is tight engagement with IT change-related projects. The architecture integrates essential elements such secure

network segmentation, intrusion detection/prevention systems, next-generation firewalls, and endpoint security solutions.

- To guarantee that security factors are incorporated from the outset, comprehensive risk evaluations are carried out, and recommendations on safe design and execution approaches are given.
- Demonstrate the team’s commitment to staying ahead of the curve by keeping a vigilant eye on emerging threats and technological advancements, which allows the team to continuously enhance HSBC UK's security posture and adapt to evolving cybersecurity challenges.

Security Operations Centre (SOC)

- Provides 24/7 monitoring of the networks, servers, apps, and endpoints of HSBC UK's IT system.
- Real-time security incident detection, investigation, and response ensures prompt threat containment and mitigation.
- Acts as a proactive defence against cyberattacks and facilitating quick action in the event of a security breach to reduce damage and safeguard the business's assets and reputation.

Furthermore, HSBC UK may engage a third-party provider for specialised security services like managed security, threat intelligence feeds, incident response support, and backup planning. For example, a cybersecurity firm such as CyberCX can provide advanced threat detection capabilities to augment the bank’s security operations. HSBC UK can strengthen its security posture, counter new threats, and rapidly address security incidents by utilising external expertise regarding to extra security protection. HSBC UK is responsible for guaranteeing that third-party providers comply with strict security standards and compliance requirements by employing robust contractual Service Level Agreements (SLAs), the network and security service provider's ability to comply with all SLAs with their customers (Peoples et al, 2021). It is a dedication to security, strengthening accountability and trust in safeguarding sensitive data and preserving operational resilience.

3 Scope

3.1 Assurance Approach

3.2 Assurance Frameworks

3.3 Scope of Security Services

HSBC (UK)

3.4 Security Services Out of Scope

4 Information Security Management System

e.g. Figure 4.1 ISO/IEC 27001:2013 control coverage

4.1.1 Certification delivery schedule

4.1.2 Risk Management

e.g. Figure 4.1.2 Risk method

e.g. Impact levels

e.g. Probability levels

4.1.3 Continual Improvement

4.1.4 Effectiveness measures

4.2 Security Testing

4.2.1 Scheduled penetration testing

e.g. Figure 4.2.1 Penetration testing schedule for Pharma University

4.2.2 Specific testing - considerations

5 Information Security Policies

e.g. Information Security policy is structured in accordance with ISO/IEC 27001:2013.

5.1 Policies and Standards

Sec.	Obj.	Control#			<description>

6 Organisation of Information Security

6.1 Operational Model

Sec.	Obj.	Control#			<description>

6.1.1 Roles and Responsibilities

6.1.2 Segregation of Duties

Sec. 5.1	Obj.	Control# 5.2.3			Control Desc

Joiners

Movers

Leavers…process?

6.1.3 Privacy by Design

Sec.	Obj.	Control#			<description>

6.2 Teleworking

Sec.	Obj.	Control#			<description>

7 Personnel Security

Sec.	Obj.	Control#			<description>

7.1 Prior to joining

7.2 During employment

7.2.1 Management Responsibilities

7.2.2 Security Training

7.2.3 Disciplinary process

7.3 Termination and Change of Employment

8 Asset Management

8.1 Responsibility for assets

Sec.	Obj.	Control#			<description>

8.1.1 Inventory of Assets

8.1.2 Ownership of assets

8.1.3 Acceptable Use of Assets

8.2 Information classification

Sec.	Obj.	Control#			<description>

8.2.1 Classification of information

Type	Description
A	?
B	
C	
D	
E	

The following table identifies further the types of data associated with each of the sub-sets identified in the previous table (if required):

Information	Pharma Universe Classification	Type	Notes
e.g. Personal information as defined by the Data Protection Act (DPA)	?	B	Protection of personal information
e.g. Sensitive personal information as defined by the Data Protection Act (DPA)	?	A	Protection of sensitive personal information. Note the more sensitive information may be marked OS
e.g. Legal privilege information	?	A or B	Treat as sensitive personal information
e.g. Witness information	?	A	Specifically sensitive; as compromise may cause personal injury. Note the more sensitive information may be marked OS

8.2.2 Labelling of information

8.2.3 Handling of assets

8.3 Media handling

Sec. ISO Ref#	Obj.?????	ISO Control#???			<description>

8.3.1 Management of Removable media

8.3.2 Disposal of media

Offiiclaly Blank

8.3.3 Physical media transfer

9 Access Control

9.1 Business requirements of access control

Sec.	Obj.	Control#			<description>

9.2 User access management

Sec.	Obj.	Control#			<description>

9.3 User responsibilities

Sec.	Obj.	Control#			<description>

9.4 System and application access control

Sec.	Obj.	Control#			<description>

9.4.1 Privileged utility programs

9.4.2 Program source code

10 Cryptography

Sec.	Obj.	Control#			<description>

10.1 Encryption of Data in Transit

Following table summarises the security controls that will be implemented to achieve data-in-transit for various solutions within PharmaUniversity.

e.g. VPN	IPsec	Securely locked on VPN gateway devices	NCSC foundation or PRIME profile
e.g. Business applications to end users	TLS 1.2	Digital certificates	NCSC assured level

10.2 Encryption of Data at Rest

10.3 Certificate and Key Management

11 Physical & Environmental Security

Sec.	Obj.	Control#			<description>

11.1 Secure Areas

•

11.2 Equipment Security

12 Operations Security

12.1 Operational procedures and responsibilities

Sec.	Obj.	Control#			<description>

12.1.1 Documented operating procedures

12.1.2 Change management

12.1.3 Capacity management

12.1.4 Separation of development, testing and operational environments.

12.2 Protection from malware

Sec.	Obj.	Control#			<description>

12.3 Backup

Sec.	Obj.	Control#			<description>

12.4 Logging and monitoring

Sec.	Obj.	Control#			<description>

12.4.1 Event Logging

12.4.2 Protection of log information

12.4.3 Clock Synchronisation

12.5 Control of operational software

Sec.	Obj.	Control#			<description>

12.6 Technical vulnerability management

Sec.	Obj.	Control#			<description>

12.6.1 Management of technical vulnerabilities

12.6.2 Restrictions on software installation

12.7 Information systems audit considerations

Sec.	Obj.	Control#			<description>

.

13 Network controls

Sec.	Obj.	Control#			<description>

13.1.1 Security of network services

13.2 Information transfer

Sec.	Obj.	Control#			<description>

13.2.1 Agreements on information transfer

13.2.2 Electronic messaging

13.2.3 Confidentiality or non-disclosure agreements

14 System Acquisition, Development and Maintenance

14.1 Security requirements of information systems

Sec.	Obj.	Control#			<description>

14.1.1 Information security requirements analysis and specification

14.1.2 Securing application services on public networks

14.1.3 Protecting applications services transactions

14.2 Security in development and support processes

Sec.	Obj.	Control#			<description>

14.2.1 Secure development policy

14.2.2 System change control procedures

14.2.3 Technical review of applications after operating platform changes

14.2.4 Restrictions on changes to software packages

14.2.5 Secure systems engineering principles

14.2.6 Secure development environment

14.2.7 Outsourced development

14.2.8 System security testing

14.2.9 System Acceptance Testing

14.3 Test data

Sec.	Obj.	Control#			<description>

HINT: From 25th May 2018 GDPR requirements also apply.

15 Supplier Relationships

15.1 Information security in supplier relationships

Sec.	Obj.	Control#			<description>

16 Information Security Incident Management

Sec.	Obj.	Control#			<description>

16.1.1 Responsibilities and procedures

There will be a security incident handling governance framework which will put overall process control in the hands of PharmaUniversity Operational Security Team.
Below is a table illustrating the identified roles and responsibilities in the process:

e.g. Operational Security Team	PharmaUniversity	?
	3rd Party?	?

16.1.2 Reporting information security events

16.1.3 Reporting information security weaknesses

16.1.4 Assessment of and decision on information security events

16.1.5 Response to information security incidents

16.1.6 Learning from information security incidents

16.1.7 Collection of evidence

17 Business Continuity

17.1 Information security continuity

Sec.	Obj.	Control#			<description>

17.1.1 Planning information security continuity

PharUniverse BCM considerations blah blah blah…..

17.1.2 Implementing information security continuity

17.1.3 Verify, review and evaluate information security continuity

17.1.4 Resilience

18 Compliance

18.1 Compliance with legal and contractual requirements

Sec.	Obj.	Control#			<description>

18.1.1 Identification of applicable legislation and contractual requirements

HINT what various legislation / acts are relevant?

18.1.1.1 General Data Protection Regulation (GDPR)

18.1.1.2 Law Enforcement Directive (LED)

18.1.2 Intellectual property rights

18.1.3 Protection of records

18.1.4 Privacy and protection of personally identifiable information

18.1.5 Regulation of cryptographic controls

18.2 Information security reviews

Sec.	Obj.	Control#			<description>

18.2.1 Independent review of information security

18.2.2 Compliance with security policies and standards

18.2.3 Technical compliance review

APPENDIX 1 – Assets

Identify two information assets of from HSBC UK (with justification)

Asset #1 – Customer Data

This asset is essential since it holds sensitive information, such as transaction history, account information, and personal data like identification numbers. Maintaining trust and adhering to data protection standards depend on the safety of protecting customer financial data.

Personally identifiable information (PII) refers to any data linked to a specific individual that can be used to determine that person's identity, such as their social security number, full name, email address, or phone number:

- A person's full name
- Mother's maiden name
- Telephone number
- IP address
- Place of birth
- Date of birth
- Geographical details (ZIP code, city, state, country, etc.)
- Employment information
- Email address or mailing address
- Race or ethnicity
- Religion

(IBM, 2024)

According to the Art 4 in Chapter 1 of GDPR, the definition of “personal data” refers to any information about a person who can be directly or indirectly identified, including a

person's name, identification number, location data, online identifier, or any other specific factors related to their physical, physiological, genetic, mental, economic, cultural, or social identity (GDPR, 2018).

By complying GDPR and PII, this is a legal requirement that HSBC has to uphold and protect the relevant customer data.

Asset #2 – Transaction Processing

Transaction Processing Systems (TPS) are a critical component of HSBC UK's infrastructure, facilitating the timely and accurate processing of financial transactions. These systems capture, process, and store transactional data from various channels, including online banking, ATM withdrawals, credit card payments, and wire transfers. The efficient operation of TPS is essential for maintaining customer satisfaction and supporting the bank's day-to-day operations, but it also plays a crucial role in ensuring regulatory compliance.

Estimation and considerations by following the FCA Handbook for the transaction processing:

- HSBC UK's TPS should implement robust operational risk management practices, including risk identification, assessment, and mitigation (FCA Handbook, SYSC 3.2)
- Transaction processing systems must comply with FCA regulations related to payment services, ensuring transparency, fairness, and security for customers (FCA Handbook, PERG 15)

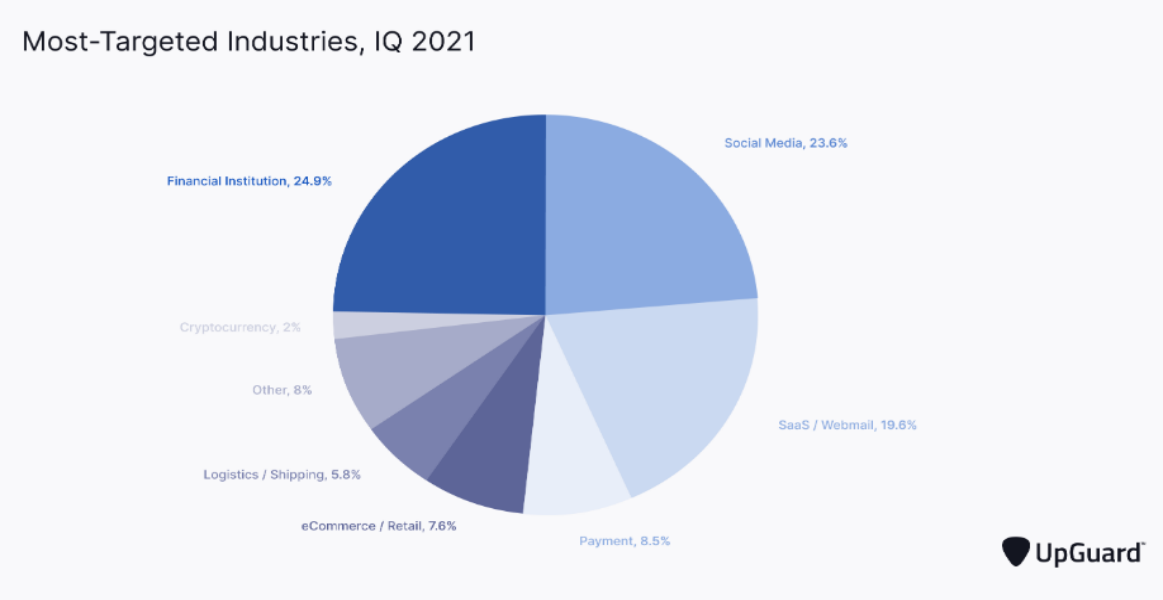
By aligning with the FCA Handbook's regulatory requirements, HSBC UK ensures compliance with industry standards and safeguards the integrity of its transaction processing operations, thereby maintaining trust and confidence among customers and stakeholders.

APPENDIX 2 – Threats

Identify industry specific threats you feel your company could be prone to (research any major breaches within HSBC UK; common threats that might impact their daily operations etc.

Threat #1 – Phishing (Upguard, 2024)

Phishing is a form of social engineering primarily conducted via deceptive emails and continues to pose a substantial threat, with email phishing being the predominant method. These emails often employ tactics such as creating a sense of urgency and hijacking existing email threads to deceive users into disclosing sensitive information. Particularly alarming is the increasing targeting of the financial sector, evidenced by a significant rise in phishing attacks, with finance being the most affected industry. Statistics reveal a consistent trend, with nearly half of all phishing attacks in 2019 aimed at financial institutions.



Threat #2 – Ransomware (Upguard, 2024)

Ransomware poses a critical cyber risk to the financial services industry, as cybercriminals increasingly target institutions to lock them out of their systems and demand ransom payments in exchange for decryption keys. These attacks have evolved to include data breach tactics, with threat actors threatening to publish sensitive information until payment is made, exploiting the heavy regulations and reputational damage concerns of financial organizations. It's essential for financial institutions to stay informed about prevalent ransomware strains to effectively defend against these threats. There are 11 most prevalent ransomware types as below:

- Sodinokibi Ransomware
- Lockbit Ransomware
- Clop Ransomware
- Egregor Ransomware
- Avaddon Ransomware
- Ryuk Ransomware
- Darkside Ransomware
- SunCrypt Ransomware
- Netwalker Ransomware
- Phobos Ransomware

Financial institutions must update their incident response plans to address these active threats to enhance their resilience against cyber threats and safeguard critical assets and sensitive data.

Threat #3 – DDoS Attacks (Upguard, 2024)

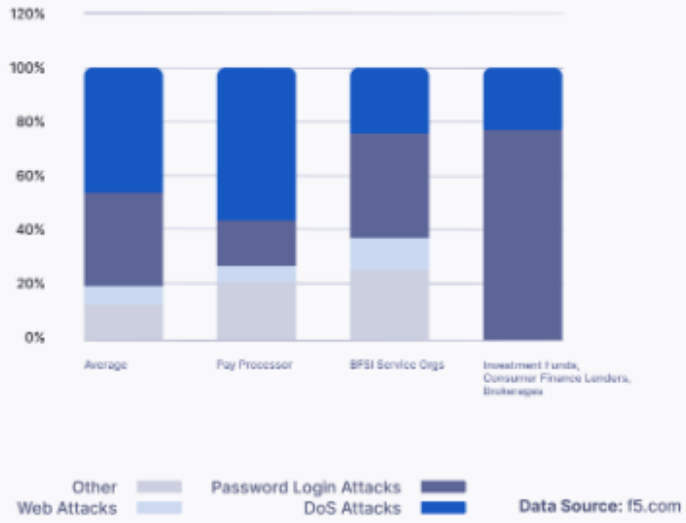
In 2020, the financial sector experienced a 30% increase in Distributed Denial-of-Service (DDoS) attacks, a significant surge compared to the previous year. These attacks targeted various aspects of the financial infrastructure, including banking IT systems, customer accounts, and payment portals. The pandemic's onset seemingly correlated with this rise in attacks. Notably, payment processes, often managed by third-party vendors associated with banks, were also heavily targeted.

Cybercriminals exploited the chaos caused by DDoS attacks in two main ways as below:

- launching additional cyberattacks while security teams were distracted and demanding ransom payments to cease the attacks.
- capitalizing on the stringent SLA agreements within the financial industry.

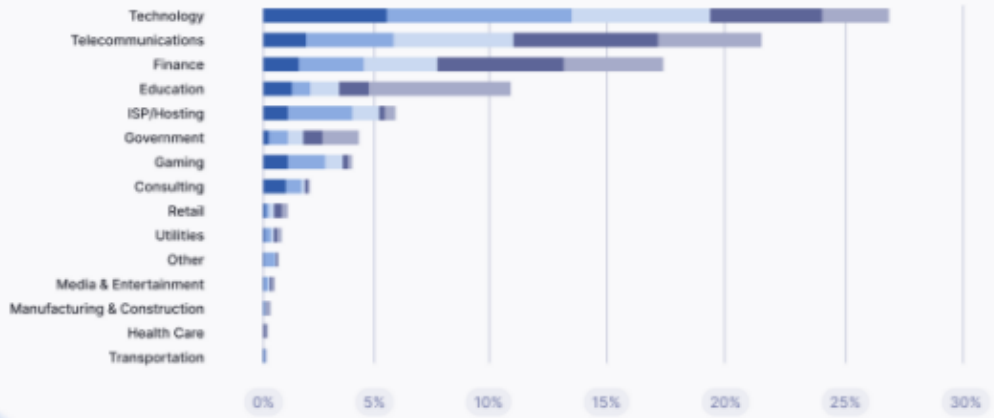
Significant threats to payment processes in 2020 included password login attacks and Denial-of-Service (DoS) attacks, according to the Data Breach Reporting Events. Between 2020 and 2021, finance consistently ranked among the top three industries targeted in Distributed Denial-of-Service (DDoS) attacks, according to the risen statistic of each industry. The result underscores the persistent threat cybercriminals pose to financial institutions, leveraging DDoS attacks to disrupt banking IT infrastructures, compromise customer accounts, and disrupt payment processes. The prevalence of these attacks highlights the ongoing need for robust cybersecurity measures within the finance sector to mitigate such threats effectively.

Data Breach Reporting Events



Data Source: f5.com

UpGuard



UpGuard

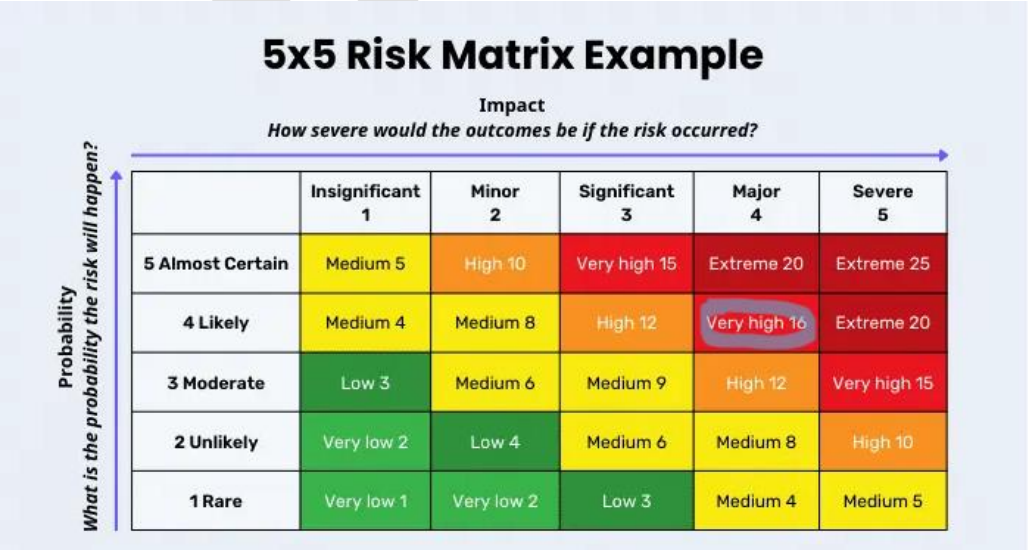
APPENDIX 3 – Risks

Five key risks to those assets (with justification and prioritisation)

Risk #1 – Data Breach Risk

(Confidentiality Impact – High; Integrity Impact – High; Availability Impact – Medium)

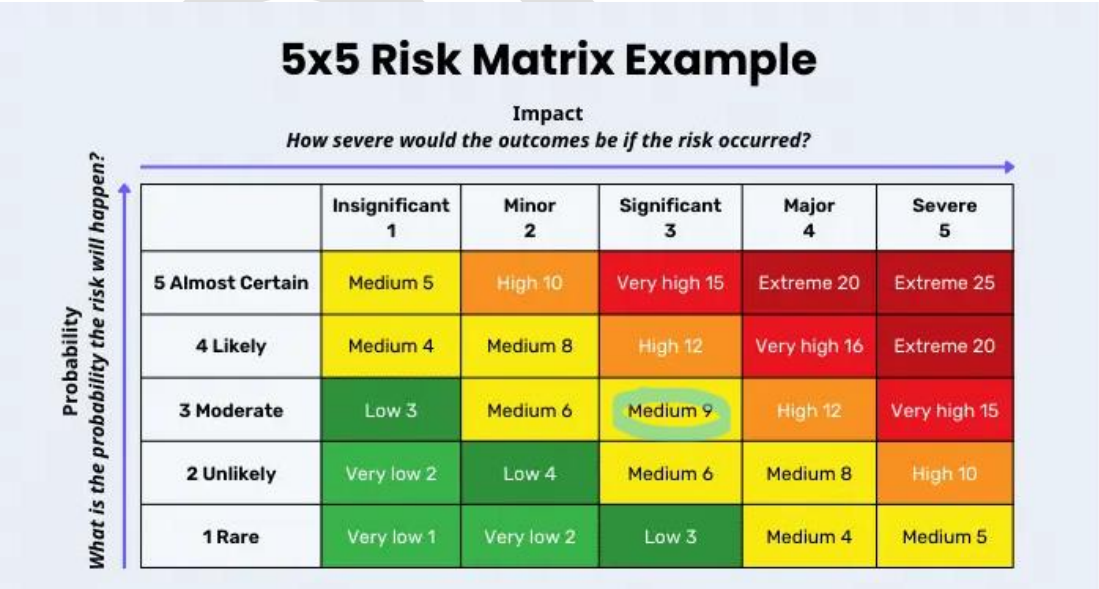
The risk of a data breach is a significant concern for protecting intellectual property assets and client financial data. Insufficient security measures, insider threats, or cyberattacks are some of the potential causes of a data breach. Breaching client financial data may result in identity theft, financial fraud, and legal issues, which can compromise the security and integrity of sensitive information. Similarly, unapproved access to intellectual property may lead to trade secret theft, reduced competitive edge, and damage to reputation. Therefore, HSBC UK takes the risk of a data breach seriously and implements strict security measures and proactive risk management techniques to ensure the security of sensitive information.



Risk #2 – Operational Disruption Risk

(Confidentiality Impact – Low; Integrity Impact – Low; Availability Impact – High)

Operational disruption poses a significant risk to the availability and continuity of banking services, impacting both customer satisfaction and financial stability. The potential consequences of cyberattacks, system failures, or natural disasters could disrupt HSBC UK's IT infrastructure, leading to service outages, transaction processing delays, and financial losses. The inability to access customer financial data or execute transactions could result in severe customer dissatisfaction, irreparable reputational damage, and intense regulatory scrutiny. Therefore, reducing operational disruption risk is crucial for business continuity and uninterrupted customer service delivery.

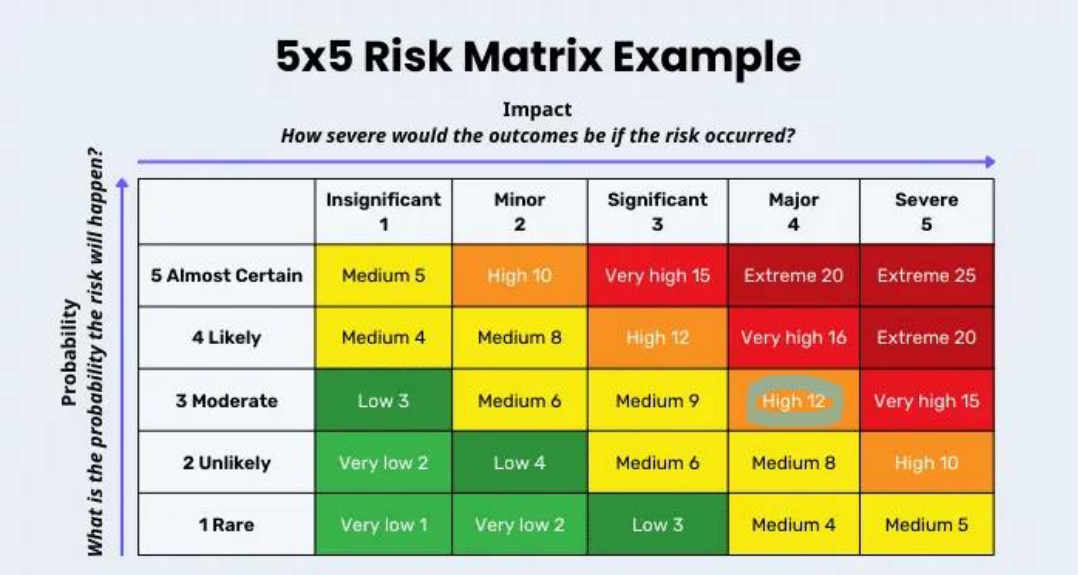


	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

Risk #3 – Reputation Risk

(Confidentiality Impact – High; Integrity Impact – Medium; Availability Impact – Low)

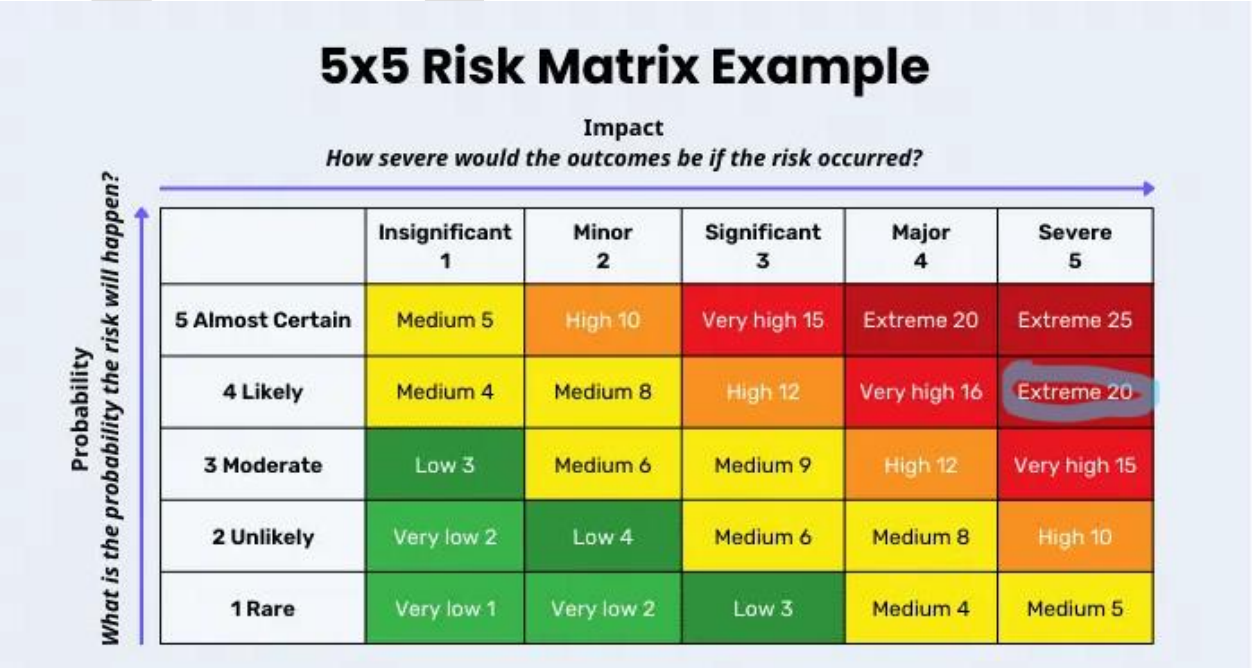
Reputation risk is persistent, emerging from the potential impact of security incidents or data breaches on HSBC UK's brand image, customer trust, and market reputation. Any adverse or negative publicity resulting from security incidents could erode customer confidence, leading to customer attrition, loss of business opportunities, and diminished market competitiveness. However, the most concerning aspect is the long-term repercussions of a damaged reputation on HSBC UK's brand equity, customer loyalty, and shareholder value. Therefore, safeguarding the bank's reputation is not just a priority; it's an immediate necessity to maintain stakeholder trust and confidence and sustain long-term business success.



Risk #4 – Online Identity Theft and Hacking Risk

(Confidentiality Impact – High; Integrity Impact – High; Availability Impact - High)

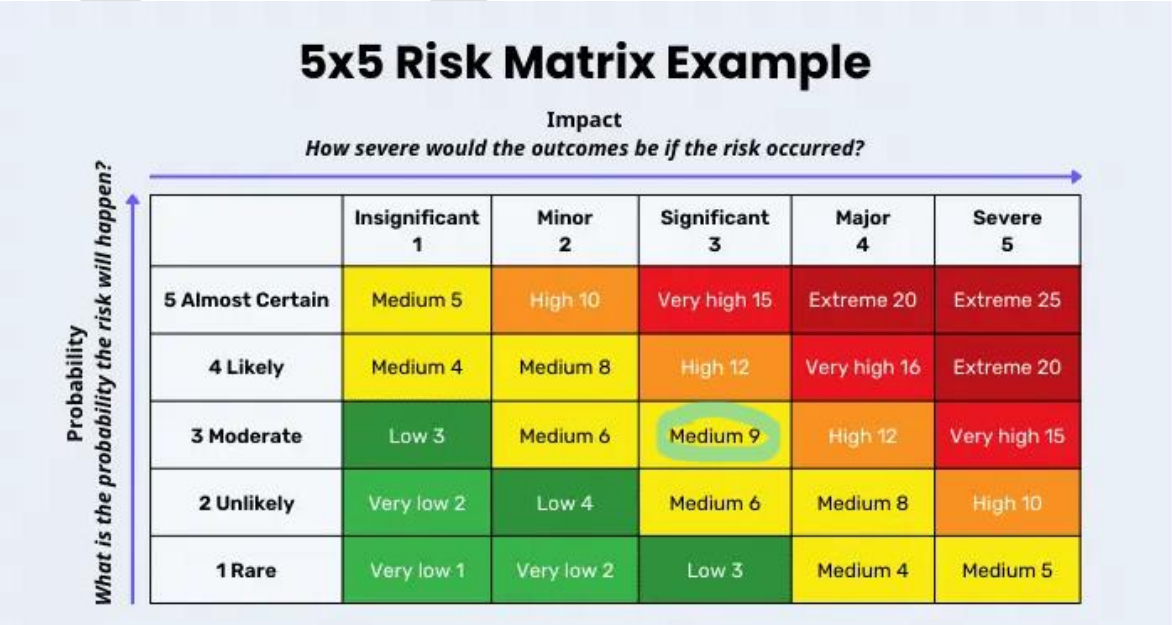
The risk of online identity theft and hacking encompasses threats related to unauthorised access to customer accounts, theft of personal information, and fraudulent activities conducted by malicious actors. Cybercriminals may exploit vulnerabilities in HSBC UK's online banking platforms, phishing attacks, or social engineering techniques to access customer accounts, compromise sensitive data, and perpetrate identity theft or financial fraud. Moreover, hacking incidents targeting HSBC UK's systems or networks could lead to service disruptions, reputational damage, and regulatory scrutiny, affecting customer trust and market confidence. Therefore, mitigating online identity theft and hacking risk requires robust authentication mechanisms, encryption technologies, and continuous monitoring to detect and prevent unauthorised access and fraudulent activities.



Risk #5 – Litigation Risk

(Confidentiality Impact – Medium; Integrity Impact – Medium; Availability Impact – Low)

Litigation risks arise from potential legal actions or regulatory penalties resulting from security incidents, data breaches, or non-compliance with regulatory requirements. Failure to protect customer financial data or intellectual property assets could expose HSBC UK to lawsuits, fines, and legal liabilities, leading to financial and economic losses and reputational damage. Moreover, litigation risks may also involve class-action lawsuits, regulatory investigations, and enforcement actions, further exacerbating the impact on the bank's operations and market reputation. Therefore, managing litigation risks requires proactive risk mitigation strategies, compliance with legal and regulatory requirements, and effective legal counsel to minimize legal exposure and safeguard the bank's interests.



APPENDIX 4 – Controls

Six controls identified from recognised industry good practice standards that will mitigate your risks (e.g. ISO27k; NIST; CE etc…)

Control #1: Encryption of Sensitive Data

Standard: **ISO/IEC 27001:2013 (Control A.18.1.3 and A.18.1.4)**

A.18.1.3 (Protection of Records): This includes robust encryption, stringent access controls, regular backups, and secure storage solutions to maintain the integrity and confidentiality of records such as customer data and intellectual property.

A.18.1.4 (Privacy and Protection of Personally Identifiable Information): This includes establishing policies and procedures for data handling, conducting privacy impact assessments, and ensuring that data processing activities comply with applicable regulations like GDPR. Specific controls include data encryption, access restrictions, consent management, and regular privacy audits.

By implementing record protection and PII privacy into the encryption strategy, HSBC UK can mitigate the risk of data breaches and unauthorised access, while also promoting a culture of data security. This ensures that all sensitive information remains secure and compliant with legal and regulatory requirements. This approach safeguards the confidentiality and integrity of sensitive data, while also addressing potential litigation risks associated with non-compliance with data protection laws.

Control #2: Multi-Factor Authentication (MFA)

Standard: **ISO/IEC 27001:2013 (Control A.9.4.2)**, **NIST SP 800-63B**

ISO/IEC 27001:2013 (A.9.4.2) (Secure log-on procedures): This control focuses on ensuring that access to information and information processing facilities is protected by secure log-on procedures. Implementing MFA can be part of these secure log-on procedures to enhance access control mechanisms.

NIST SP 800-63B: This provides detailed guidelines for implementing digital identity and authentication processes, emphasizing the importance of MFA for securing access to information systems.

Implement multi-factor authentication (MFA) for employee and customer access to online banking platforms and internal systems. MFA adds an extra layer of security by requiring users to provide multiple verification forms before granting access. This significantly reduces the risk of unauthorised account access and identity theft, making the systems more secure. By implementing MFA, HSBC UK can strengthen authentication controls, further reducing the risk of online identity theft and unauthorised access to sensitive data. This, in turn, enhances the security of customer accounts and internal systems, providing a higher level of security. Using recognised standards like ISO/IEC 27001, PCI DSS, and NIST ensures that MFA implementations are robust, compliant, and aligned with industry best practices, reinforcing the effectiveness of our security measures and making the clients feel secure about the proposed changes.

Control #3: Intrusion Detection and Prevention Systems (IDPS)

Standard: **ISO/IEC 27001:2013 (Control A.12.6.1)**, **NIST SP 800-53 (Control SI-4)**, **CIS Controls v8 (Control 13)**

ISO/IEC 27001:2013 (A.12.6.1): This control is of utmost importance as it focuses on ensuring that information about technical vulnerabilities is obtained and the organization's exposure to such vulnerabilities is evaluated and appropriately addressed.

NIST SP 800-53 (Control SI-4): System and Information Integrity - Intrusion Detection Systems. This control, which is a crucial requirement, mandates organizations to implement network-based and host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor and analyse events to detect attacks and potential intrusions.

CIS Controls v8 (Control 13): Data Protection - Implement network-based and host-based intrusion detection tools to identify and alert on malicious behaviour. Ensure these tools are configured to detect known attack signatures, abnormal traffic patterns, and other indicators of potential compromise. For instance, 'known attack signatures' refer to specific patterns of data that are indicative of a particular type of attack, while 'abnormal traffic patterns' could include a sudden surge in network traffic or a high volume of requests from a single IP address.

Deploying intrusion detection and prevention systems (IDPS) to monitor network traffic, detect suspicious activities, and prevent unauthorised access or malicious attacks is crucial for enhancing an organisation's ability to respond to threats effectively. By implementing IDPS according to comprehensive standards, HSBC UK can detect and prevent potential cyberattacks, thus reducing the risk of operational disruption and unauthorised access to critical systems and data. These systems enhance overall security by providing real-time alerts and automated responses to threats, ensuring continuous monitoring and protection of the IT environment.

Control #4: Incident Response Plan and Business Continuity Planning (BCP)

Standard: **ISO/IEC 27001:2013 (Control A.16.1.1)**, **ISO 22301 Business Continuity Management**

ISO/IEC 27001:2013 (Control A.16.1.1): This control is a crucial component of ISO standards, which are vital in security and business continuity management. It establishes incident management procedures to ensure a timely and effective response to security incidents, including processes for reporting incidents, assessing their impact, containing and eradicating threats, and recovering from incidents.

ISO 22301 Business Continuity Management: This standard is a comprehensive guide for implementing and maintaining a business continuity management system. It covers the development of a comprehensive business continuity plan, including risk assessments, business impact analyses, recovery strategies, and continuity plans. These measures ensure the organization can continue essential functions during disruptions, making it a reliable resource for business continuity.

Develop and implement an incident response plan and business continuity plan to ensure a coordinated and effective response to security incidents and disruptions to

business operations. Robust incident response and business continuity capabilities minimise the impact of security incidents and operational disruptions, enabling swift recovery and continuity of essential services, thereby reducing financial losses and reputational damage.

Control #5: Regular Security Assessments and Audits

Standard: **ISO/IEC 27001:2013 (Control A.12.1.2)**, **NIST SP 800-53 Rev. 5**, **CIS Controls v8 (Control 1)**, **COBiT 2019 (DSS05.02)**

ISO/IEC 27001:2013 (A.12.1.2): This control emphasizes the importance of regular reviews and audits of the ISMS to ensure its effectiveness and compliance with security policies and objectives.

NIST SP 800-53 Rev. 5: This control requires organizations to conduct periodic assessments of the security controls to ensure they are implemented correctly, operating as intended, and meeting the organization's security requirements.

CIS Controls v8 (Control 1): Inventory and Control of Enterprise Assets. This control emphasizes the importance of maintaining an inventory of authorized and unauthorized devices, software, and other assets to ensure they are properly managed and secured.

COBIT 2019 (DSS05.02): Perform Data Security Assessments. This control requires organizations to conduct regular data security assessments to identify and mitigate risks related to data confidentiality, integrity, and availability.

Regular security assessments and audits should be conducted to evaluate the effectiveness of security controls, identify vulnerabilities, and address compliance gaps. These measures help HSBC UK proactively identify and rectify security vulnerabilities, compliance issues, and risks, ultimately enhancing overall security and reducing the likelihood of security incidents and data breaches.

Control #6: Security Awareness Training

Standard: **ISO/IEC 27001:2013 (Control A.7.2.2)**

A.7.2.2: All organization employees and, where relevant, contractors are required to receive appropriate awareness education and training. Equally important, they should also be regularly updated on organizational policies and procedures that are relevant to their job function. This ensures that everyone is well-informed about the latest security measures and can contribute to maintaining a secure environment.

The control requires organizations to provide regular security awareness training to all employees, contractors, and third-party users. This training is designed to increase their understanding of information security risks, policies, procedures, and best practices, empowering them to handle security threats effectively.

By implementing this control, HSBC UK can empower its employees to become active participants in the organisation's security efforts, reducing the risk of insider threats, human errors, and security incidents. Security-aware employees are better equipped to identify and report suspicious activities, adhere to security policies and procedures, and protect sensitive information from unauthorised access or disclosure. This contributes to a culture of security within the organisation, enhancing its overall security posture and resilience to cyber threats.

APPENDIX 5 – Estimated Effectiveness

Estimated effectiveness demonstrating ‘qualitative’ and ‘quantitative’ means (showing reduction in your perceived risk before and after implementing your control(s)

Qualitative risk analysis: The organisation uses ordinal rating scales to assess risks based on how likely they are to occur and their impact. This allows for a visual representation of their relative severity. However, this approach needs improvement, especially in terms of consistency. As it relies on subjective judgments, assessors may need to clearly define the parameters of their assessments, leading to an unclear understanding of risk and potentially inconsistent evaluations.

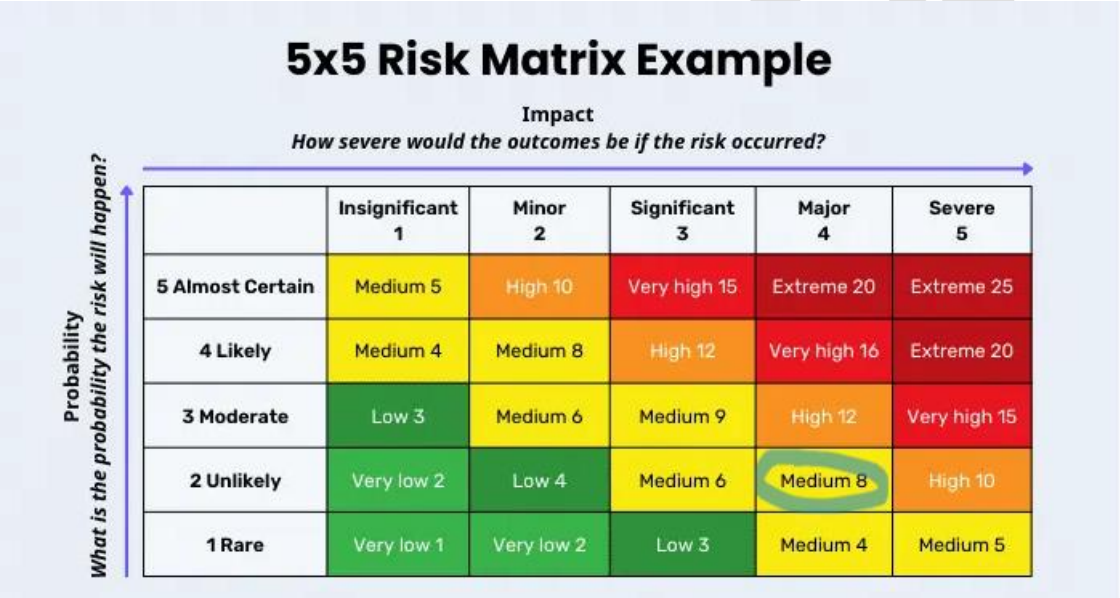
Quantitative risk analysis: It effectively mitigates biases and inconsistencies with a well-defined risk evaluation model. Moreover, it resolves the prioritisation challenge by employing economic metrics, specifically pounds and pence, as its measurement rather than relying on ordinal or relative scales.

Risk #1 – Data Breach Risk

- **Controls Implemented:**
- **Encryption of Sensitive Data**
- **Intrusion Detection and Prevention Systems (IDPS)**

Before the implementation: Without encryption and adequate protection measures, sensitive data is vulnerable to unauthorised access. Lack of intrusion detection increases the risk of undetected breaches.

After the implementation: Implementing encryption, protection controls, and IDPS significantly minimizing unauthorized access and boosting detection capabilities lowers the risk of data breaches.



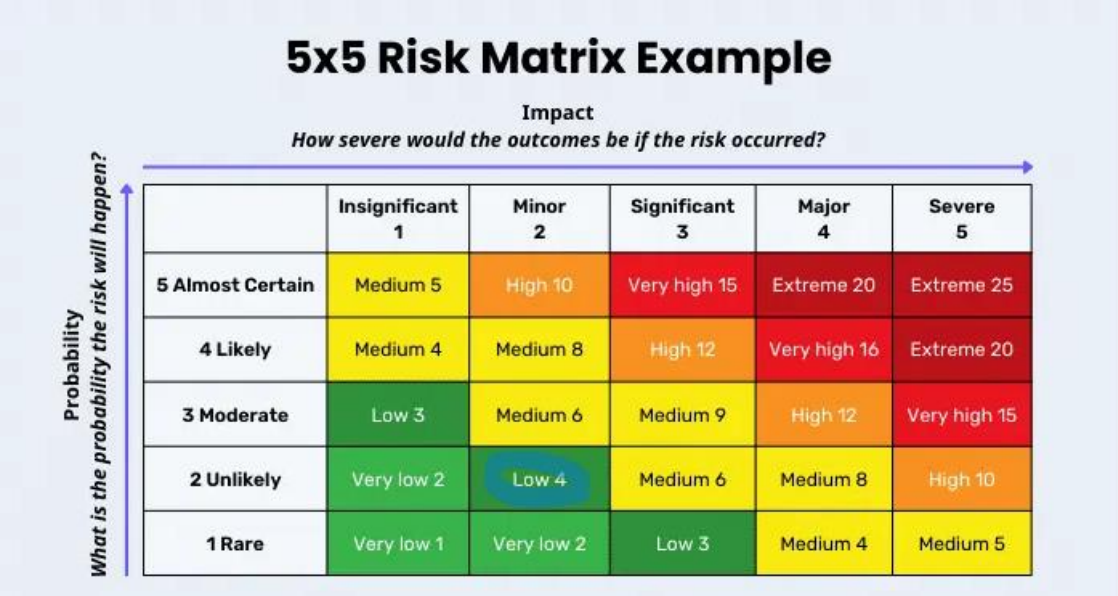
Risk #2 – Operational Disruption Risk

Controls Implemented:

- **Incident Response Plan and Business Continuity Planning**
- **Regular Security Assessments and Audits**

Before the implementation: Lack of a structured incident response plan and business continuity strategy raises the risk of operational disruptions and delays in restoring services. Insufficient security assessments might overlook important vulnerabilities.

After the implementation: Developing an incident response plan and business continuity strategy and regular security assessments enhances and the organisation's ability to withstand disruptions, allowing for quick detection, containment, and recovery from incidents.



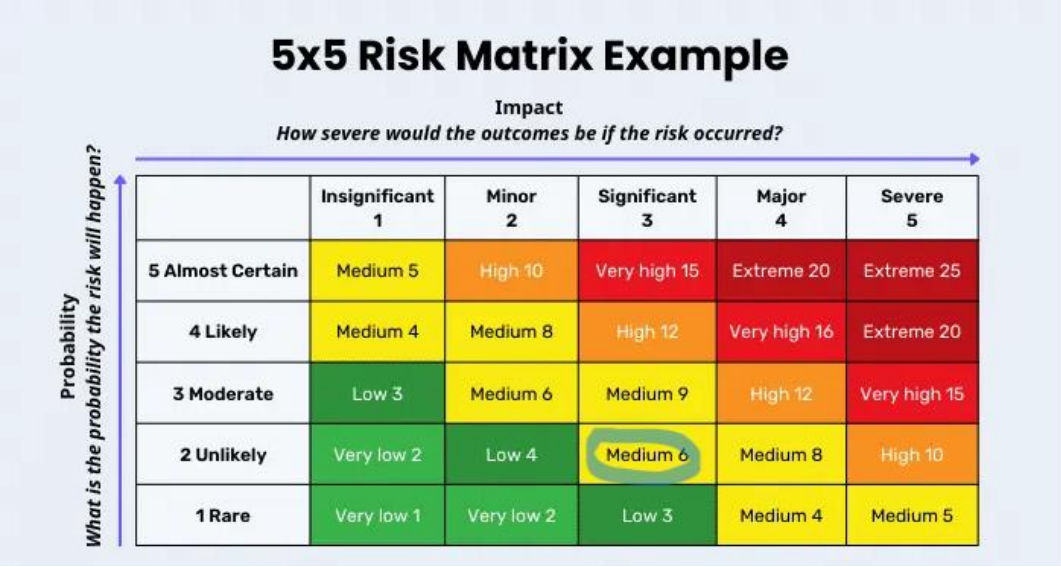
Risk #3 – Reputation Risk

Control Implemented:

- **Security Awareness Training**
- **Incident Response Plan and Business Continuity Planning**

Before the implementation: Lack of employee awareness increases the risk of security incidents and reputational damage due to insider threats or potentially human errors.

After the implementation: Providing comprehensive security awareness training and implementing incident response plans enhance the organization's ability to mitigate security incidents and safeguard reputation.



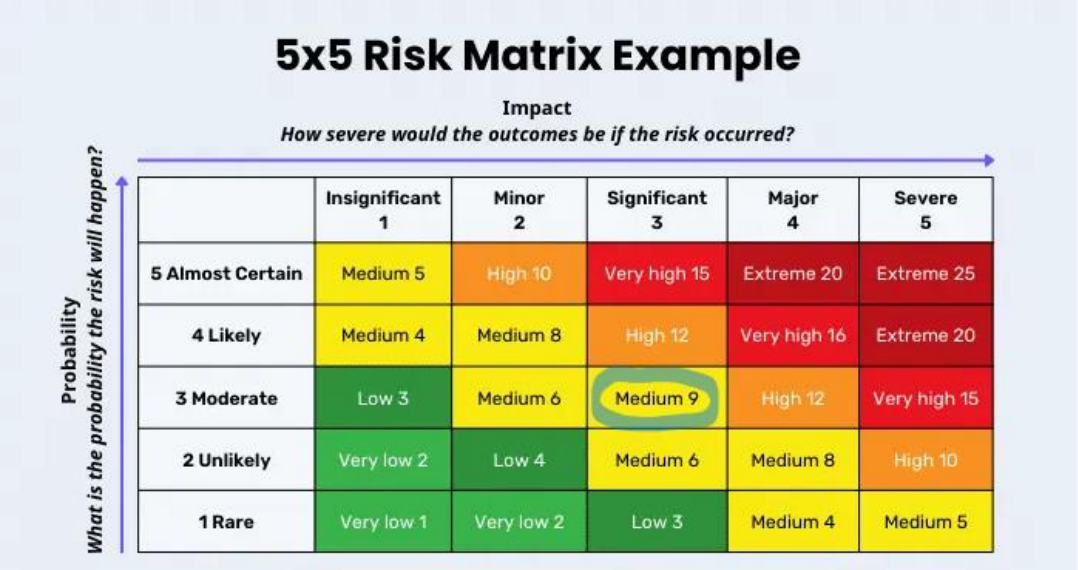
Risk #4 – Online Identity Theft and Hacking Risk

Controls Implemented:

- **Multi-Factor Authentication (MFA)**
- **Intrusion Detection and Prevention Systems (IDPS)**

Before the implementation: Weak authentication mechanisms and lack of intrusion detection increase vulnerability to online identity theft and hacking attempts.

After the implementation: By implementing MFA and IDPS, security is enhanced through an additional layer of authentication and improved detection capabilities, reducing the likelihood of successful hacking attempts.



Risk #5 – Litigation Risk

Controls Implemented:

- **Regular Security Assessments and Audits**
- **Encryption of Sensitive Data**

Before the implementation: Inadequate security assessments and lack of data encryption increase vulnerability to non-compliance and litigation risks.

After the implementation: Conducting regular security assessments, data encryption, and protection controls ensure compliance with legal requirements, reducing the risk of litigation and legal liabilities.

5x5 Risk Matrix Example

Impact

How severe would the outcomes be if the risk occurred?

What is the probability the risk will happen?

Probability

	Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
5 Almost Certain	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
4 Likely	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
3 Moderate	Low 3	Medium 6	Medium 9	High 12	Very high 15
2 Unlikely	Very low 2	Low 4	Medium 6	Medium 8	High 10
1 Rare	Very low 1	Very low 2	Low 3	Medium 4	Medium 5

APPENDIX 6 – Key Barriers

Your key barriers/challenges to implementation of each control you have identified

Barrier / Challenges of Encryption of Sensitive Data

The crucial barrier to implementing encryption of customer data is the potential impact on system performance and usability. While essential for data security, robust encryption algorithms may introduce processing overhead and latency, significantly affecting the speed and responsiveness of banking systems and customer transactions.

Alternative Approach: Optimised encryption algorithms and hardware acceleration optimisation technologies can significantly improve performance impact while ensuring robust data security. This approach offers a promising solution to the encryption challenges.

While optimisation algorithms can mitigate performance overhead, they may compromise the encryption strength and resilience against advanced cryptographic attacks (Singh et al, 2017). Therefore, balancing effectiveness with ease of implementation requires meticulous consideration of performance requirements and security objectives. Organisations can balance encryption strength and performance by leveraging hardware-based encryption solutions and adopting encryption technologies optimised for specific use cases. The trade-offs between encryption effectiveness and ease of implementation should be carefully evaluated. This evaluation ensures that security measures do not impact system performance or user experience.

Barriers / Challenges of Multi-Factor Authentication (MFA)

Employee resistance to adopting MFA due to perceived inconvenience and usability issues may hinder implementation efforts. Some employees may also resist using additional authentication factors, viewing them as cumbersome or time-consuming, which could lead to non-compliance and security gaps.

Alternative Approach: Implementing user-friendly MFA solutions, which provide seamless authentication experiences and support multiple authentication methods like biometrics, smart cards, or mobile authentication apps, can significantly improve usability and convenience, and drive higher employee adoption rates.

User-friendly MFA solutions can improve usability and employee adoption rates. However, it's important to take into account their preferences. These solutions may add complexity and management overhead for IT administrators. Therefore, achieving a balance between effectiveness and ease of implementation involves considering user preferences, security requirements, and administrative capabilities. Organisations can boost MFA adoption rates by providing flexible authentication options and implementing user-centric authentication workflows (Sinigaglia et al, 2020). Therefore, it can enhance MFA effectiveness by addressing usability concerns and offering diverse authentication methods while reducing employee resistance.

Barriers / Challenges of Intrusion Detection and Prevention Systems (IDPS)

Challenges with integrating IDPS solutions and dealing with false positive alerts can impede effective implementation and operational efficiency. IDPS solutions often need customisation and fine-tuning to align with organisational networks and security policies. Additionally, false positives can overwhelm security teams and lead to alert fatigue.

Alternative Approach: Implement machine learning-based IDPS solutions that can automatically adapt to evolving threats and network conditions, reducing the need for manual configuration and tuning.

As machine learning-based IDPS solutions offer improved detection accuracy and adaptive capabilities, they may require sophisticated expertise and resources for deployment and maintenance. Additionally, reliance on AI-based algorithms may

introduce risks of evasion techniques and adversarial attacks. Organisations can improve the effectiveness of IDPS solutions by using machine learning and AI technologies to enhance threat detection and reduce false favourable rates (Hassan and Ibrahim, 2023). However, they must also weigh the trade-offs related to complexity, resource requirements, and potential vulnerabilities associated with AI-based security solutions.

Barriers / Challenges of Incident Response Plan and Business Continuity Planning

Lack of senior leadership buy-in and organisational support for incident response and business continuity planning may undermine the effectiveness of preparedness efforts. Without active engagement and commitment from senior management, incident response plans and business continuity strategies may lack sufficient resources, visibility, and authority to be implemented effectively.

Alternative Approach: To establish a dedicated incident response and business continuity team with clear roles, responsibilities, and authority to coordinate response efforts and ensure alignment with organisational objectives. Regular tabletop exercises and simulations should be conducted to test plans' effectiveness and identify areas for improvement.

While dedicated incident response teams and tabletop exercises can enhance preparedness and response capabilities, they may require additional investments in training, staffing, and infrastructure. Moreover, achieving consensus and buy-in from stakeholders across the organisation may pose challenges. Organisations can improve incident response and business continuity preparedness by establishing dedicated teams and conducting regular exercises to validate plans and enhance coordination (Blyth, M., 2009). By fostering a culture of resilience and accountability, organisations can overcome barriers related to leadership buy-in and organisational support for incident response and business continuity planning.

Barriers / Challenges of Regular Security Assessments and Audits

Resource constraints and compliance fatigue may impede the frequency and thoroughness of security assessments and audits. Limited budget and staffing resources may restrict the organisation's ability to conduct comprehensive evaluations and audits regularly, leaving security vulnerabilities undiscovered or unaddressed.

Alternative Approach:

Adopt risk-based approaches to prioritise security assessments and audits based on the criticality of assets and the likelihood of threats. Implement automated tools and technologies to monitor and assess security controls continuously to supplement periodic audits. Matheu-García,2019

The use of risk-based approaches and automation can enhance resource allocation and boost efficiency in security assessments. However, these methods may fail to identify specific vulnerabilities or emerging threats that require manual intervention or expert analysis. Additionally, relying solely on automated tools may lead to false negatives and misconfiguration risks. Organisations can achieve greater efficiency and effectiveness in security assessments by adopting risk-based approaches and leveraging automation technologies for continuous monitoring (Matheu-García et al, 2019).To concentrate on high-risk areas and automating repetitive tasks, organisations can overcome resource limitations and compliance fatigue while upholding a strong security posture.

Barriers / Challenges of Security Awareness Training

The challenge of effectively implementing security awareness training for employees lies in measuring its impact on behaviour change and adherence to security policies. Despite organisations investing resources in delivering training sessions, assessing the effectiveness of improving employees' cybersecurity awareness and reducing security incidents remains a challenge.

Alternative Approach: Implement interactive and gamified training modules to engage employees and make cybersecurity learning fun and interactive. Use real-world examples and case studies to illustrate the importance of security practices in protecting sensitive information.

While interactive training approaches can enhance employee engagement and knowledge retention, they may require additional time and resources for development and delivery. Moreover, measuring the effectiveness of gamified training methods and their impact on behavior change may pose challenges. Interactive and gamified training approaches can improve employee engagement and knowledge retention in cybersecurity awareness programs (Faith et al, 2024). By making training sessions more interactive and relevant to employees' daily tasks, organisations can enhance the effectiveness of security awareness training while overcoming barriers related to engagement and participation.

Reference

1. HSBC, 2024. https://www.hsbc.com/who-we-are/our-history
2. Buckley, R.P., Zetzsche, D.A., Arner, D.W. and Tang, B.W., 2021. Regulating artificial intelligence in finance: Putting the human in the loop. Sydney Law Review, The, 43(1), pp.43-81.
3. Trudeau, C. and McLarney, C., 2017. How Can Banks Enhance International Connectivity with Business Customers?: A Study of HSBC. *IUP Journal of Business Strategy*, *14*(2).
4. Merhi, M., Hone, K. and Tarhini, A., 2019. A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust. Technology in Society, 59, p.101151.
5. Powley, H. and Stanton, K., 2020. Financial conduct in the UK's banking sector: Regulating to protect vulnerable consumers. In Discrimination, Vulnerable Consumers and Financial Inclusion (pp. 206-235). Routledge.
6. FCA Final Notice, 2023. https://www.fca.org.uk/publication/final-notices/equifax-limited-2023.pdf
7. FCA News, 2021. https://www.fca.org.uk/news/press-releases/fca-fines-hsbc-bank-plc-deficient-transaction-monitoring-controls
8. Gulyás, O. and Kiss, G., 2023. Impact of cyber-attacks on the financial institutions. Procedia Computer Science, 219, pp.84-90.
9. Guardian, 2016. https://www.theguardian.com/money/2016/jan/29/hsbc-online-banking-cyber-attack
10. Ashish Khaitan, 2024. https://thecyberexpress.com/hsbc-bank-data-breach-barclays/
11. Peoples, C., Rafferty, J., Moore, A. and Zoualfaghari, M., 2021. Managing Cybersecurity Events Using Service-Level Agreements (SLAs) by Profiling the People Who Attack. In Advances in Cybersecurity Management (pp. 221-243). Cham: Springer International Publishing.
12. GDPR, 2018. https://gdpr-info.eu/
13. IBM, 2024. https://www.ibm.com/topics/pii
14. Upguard, 2024. https://www.upguard.com/blog/biggest-cyber-threats-for-financial-services
15. Taylor Maze, 2018. https://www.fairinstitute.org/blog/qualitative-vs.-quantitative-analysis-for-cyber-risk-whats-the-difference
16. Singh, S., Sharma, P.K., Moon, S.Y. and Park, J.H., 2017. Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. Journal of Ambient Intelligence and Humanized Computing, pp.1-18.

17. Sinigaglia, F., Carbone, R., Costa, G. and Zannone, N., 2020. A survey on multi-factor authentication for online banking in the wild. Computers & Security, 95, p.101745.
18. Hassan, S.K. and Ibrahim, A., 2023. The role of artificial intelligence in cyber security and incident response. International Journal for Electronic Crime Investigation, 7(2).
19. Blyth, M., 2009. Business continuity management: building an effective incident management plan. John Wiley & Sons.
20. Matheu-García, S.N., Hernández-Ramos, J.L., Skarmeta, A.F. and Baldini, G., 2019. Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices. Computer Standards & Interfaces, 62, pp.64-83.
21. Faith, B.F., Long, Z.A. and Hamid, S., 2024, May. Promoting cybersecurity knowledge via gamification: an innovative intervention design. In 2024 Third International Conference on Distributed Computing and High Performance Computing (DCHPC) (pp. 1-8). IEEE.