Cybersecurity Governance, Risk and Compliance

Year 2 Semester 4

SCHOOL OF INFOCOMM TECHNOLOGY

Diploma in Cyber Security & Digital Forensics

ASSIGNMENT

Tutorial Group: **T04**

Tutor: **Mr Fabien NG**

Date of Submission: ______________________

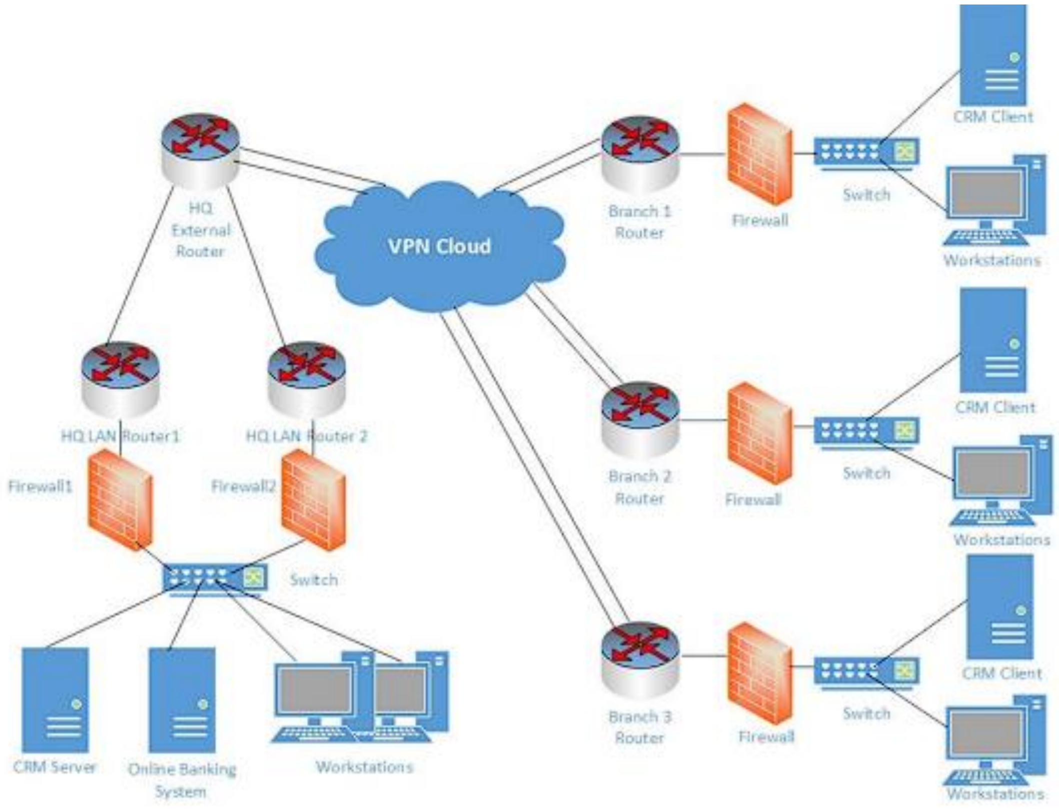
Student Number	Student Name	Grade
S10258382	Ivan Ng Keyang	
S10258107E	Gan Jun Hang	
S102241798G	Pooh Wen Kang Ethan	
S10259970K	Teo Jun Heng	
S10257500G	Raphael Low Keen Wai	

Table of Contents

Background and Context

This report aims to address the increasing threat landscape faced by DGT Bank and the protection of sensitive information stored in their systems. The report will cover the various threats and their corresponding risks associated with each critical company asset. Moreover, proposed measures and guidelines will be designed such that implementation of these suggested measures will not only bolster DGT Bank's defenses against cyber threats but also reinforce its commitment to customer loyalty, shareholder value, and employee satisfaction. The report will ensure that its focus would be aligning the bank’s cybersecurity initiatives with its mission and vision such that DGT Bank can continue to thrive in a rapidly evolving digital landscape while maintaining, if not further enhancing the trust and confidence of all stakeholders

Network Diagram



Risk Management Plan

Risk management involves the identification, analysis and remedy of highlighted risks associated with every asset within the company. This section breaks down this process into three parts; Identification, Assessment and Control.

Risk Identification

Critical information

As DGT is a global financial institution, there must be a lot of important information that they try to protect.

1. Customer Information

The first of which is customer information. In order to establish a strong reputation and trust with their customers, DGT must carefully handle and manage their customer's information. If this critical information somehow gets leaked, there would be major consequences. To narrow down the scope of these consequences, we will separate them into these 4 categories.

1.1 Reputational Damage

Loss of Customer Trust – The first and most obvious would be reputational damage. With how many financial institutions rely heavily on trust, a data breach would erode customer confidence near instantly, leading to customer attrition as clients move to companies with stronger, better and more secure reputations.

Public Relations Challenges – Reputational damage is typically not easily fixed. This long and painstaking effort often requires aggressive PR efforts, which a company may not have after suffering reputational damage as it is costly and time consuming. Additionally, negative media coverage will only serve to further hurt public perception of the company.

1.2 Legal and Regulatory Consequences

Fines and Sanctions – Regulatory bodies like the GDPR in Europe, CCPA in California, and others worldwide impose heavy fines for data breaches. These penalties can reach millions or even billions of dollars, depending on the severity.

Legal Actions and Settlements – Customers whose data has been leaked may file lawsuits. Financial institutions often face class-action lawsuits in the wake of major leaks, leading to settlements or prolonged legal battles. This would cause major stress to the PR team of DGT should this happen. An example of this would be MGM, who, in the past, had to pay $45 Million to settle a Data-Breach lawsuit.

Increased Regulatory Scrutiny – After a data breach, the financial institution may be subjected to additional audits and oversight, tightening regulations on how they handle data. And the existing regulations would be heavily re-examined to ensure that the existing measures are good enough.

1.3 Financial Impact

Direct Financial Loss – Beyond fines, there are costs related to investigating the breach, notifying affected customers, and possibly compensating for the damages.

Increased Insurance Premiums – Cyber insurance premiums often rise after a data breach, adding to the institution’s ongoing operational costs.

Market Value and Investor Confidence – Data breaches often lead to a drop in stock prices as investor confidence wanes. Financial markets react negatively to such events, particularly with major institutions, affecting long-term valuations.

1.4 Operational and Cybersecurity Overhaul

Incident Response and Forensics – After a breach of customer information, an institution must investigate how the breach initially occurred. This includes what data was accessed and how vulnerabilities were exploited in the first place. This usually involves engaging cybersecurity firms and specialists, which can be quite costly, especially with the decline of clients after a breach.

Enhanced Security Measures – Financial institutions like DGT often upgrade or overhaul their security infrastructure post-breach, implementing stricter data access policies, encryption, regular audits, and employee training programs. (*Empowering and Securing Banking and Financial Organizations*, 2023)

Operational Disruption – Internal resources may be re-allocated to address the breach, which will affect regular operations. In severe cases, the organisation might temporarily suspend certain services to prevent certain data exposure. This will in turn cause further loss of revenue and customers to become increasingly frustrated with the company, causing a negative overall reaction. (Gammon, 2025)

2. Financial Transaction Data

Another piece of critical information that cannot leave DGT is financial transaction data. Financial transaction data may be even more dangerous than allowing customer information to leak. And this is because financial transaction data can contain things like the full name, or legal address of a customer (via the billing address). Additionally, having access to other people’s financial transaction data also means that someone may perform identity theft and purchase things using a victim’s card information.

3. Third-Party and Vendor Information

Additionally, third party and vendor information are also important pieces of information that should never leave the confines of a financial institution. Information about contracts with third-party vendors and suppliers could contain pricing information, terms of service, and service-level agreements that could be advantageous to competitors or misused by threat actors.

4. Employee Information

Next, Employee Information is also a critical piece of information that must be kept confidential. Again, a similar flow of logic can be applied for employee information like how customer information should not leave the company walls. There would be people committing lots of fraudulent efforts everywhere.

5. Intellectual Property and Trade Secrets

And finally, Intellectual Property and Trade Secrets. It is pretty obvious why one should not allow these secrets to leak, as it will lead to competitive disadvantages if other companies know what your company knows. It allows other companies to bolster the knowledge they didn’t have on top of having an advantage over your company as they have their own trade secrets. And financial institutions often use proprietary software for trading, risk analysis, fraud detection, and client management. Leakage of these algorithms could lead to competitive disadvantages. Any ongoing projects or planned services should be kept confidential to prevent competitors from copying ideas or gaining market advantages. Information about investment algorithms, trading strategies, or portfolio management tactics should be protected to avoid manipulation or theft by competitors or malicious actors. (Team C, n.d.)

6. Customer Behavioral and Analytics Data

Behavioural and analytics data are also highly sensitive and require stringent protection. This data includes insights into customer spending habits, transaction patterns, and financial preferences, which financial institutions like DGT often use to offer tailored products and services. If leaked, this information could be weaponized for targeted phishing attacks or fraud, putting customers at serious risk. Moreover, competitors could use this data to gain an unfair advantage by mirroring or preempting DGT's business strategies. (Stevenwoodson, 2024)

7. Unreleased Financial Products or Services

Protecting information about upcoming financial products and services is crucial for maintaining a competitive edge. This type of information often includes details about product designs, pricing models, and launch strategies. If this data were leaked, competitors could launch similar or more aggressive alternatives, severely undercutting DGT's plans. Such breaches could also lead to reputational damage, as customers may question the institution's ability to keep strategic information confidential. (Team C, n.d.)

8. Online Banking Information

Another critical area DGT must prioritize is the protection of online banking information. This encompasses not only user credentials and transaction records but also systems that facilitate real-time payment platforms like PayNow and other similar services. A breach in these systems could result in unauthorized transfers or theft, causing both financial loss and a significant blow to customer confidence. Given how integral online banking is to modern financial services, especially with seamless payment integrations like PayNow and FAST (Fast and Secure Transfers), protecting this data is paramount. Cybercriminals are continually targeting these platforms because of the direct access they provide to financial resources. Moreover, a compromise in this area could lead to severe penalties under Singapore's strict financial regulations, such as those outlined in the Payment Services Act, and irreparable damage to DGT's reputation. By ensuring safeguards for online banking systems, DGT can continue to provide secure and reliable digital payment solutions that customers can trust. (Koch, 2024)

9. CRM Server Information

Protecting CRM (Customer Relationship Management) server information is absolutely critical for DGT. These systems store large amounts of customer-related data, including personal details, financial records, and communication histories. A breach could spell trouble, with sensitive information falling into the wrong hands which would lead to identity theft, fraud, or other forms of misuse. The fallout wouldn't stop there, as it could expose DGT to severe legal and regulatory penalties while violating confidentiality. On top of that, these servers are the backbone of customer interactions, playing a critical role in maintaining relationships and ensuring seamless communication. Any unauthorised changes or loss of data could disrupt client services, leaving customers frustrated and eroding trust in DGT's dependability. Securing these servers isn't just about protecting data; it's essential for keeping operations running smoothly and reinforcing DGT's reputation as a trusted, customer-focused institution. (Clifton, 2024)

10. External Firewall

The external firewall acts as the first line of defense between DGT's network and the internet, filtering incoming and outgoing traffic to block unauthorized access. It protects against external threats such as DDoS attacks, malware, and intrusion attempts by inspecting network packets and enforcing security policies. If compromised, attackers could bypass perimeter defenses and gain access to DGT's internal network, leading to data breaches or service disruptions. Ensuring proper firewall configuration, rule enforcement, and continuous monitoring is critical to safeguarding the organization from external cyber threats.

11. Internal Firewall

The internal firewall is designed to segregate and protect different internal network segments, such as separating the CRM system, online banking system, and workstation networks. It enforces access controls and traffic filtering to prevent lateral movement of threats within the organization. Without a properly secured internal firewall, an attacker who breaches the external defenses could move freely between systems, potentially compromising customer data, financial transactions, and administrative controls. Implementing least privilege access, network segmentation, and real-time monitoring helps ensure that even if an attacker gains a foothold, the spread of the attack is minimized.

12. VPN

The VPN ensures secure, encrypted communication between remote users and DGT's internal network. If compromised, an attacker could intercept sensitive information such as login credentials, financial data, or transaction details. A breached VPN also opens the door to unauthorized access to internal systems, allowing attackers to infiltrate the network, exfiltrate data, or disrupt operations. As remote work is increasingly common, a vulnerable VPN could significantly heighten DGT's exposure to cyber threats, potentially leading to large-scale data breaches and financial fraud. (*Empowering and Securing Banking and Financial Organizations*, 2023)

13. Cloud Infrastructure

DGT's cloud infrastructure is critical for hosting sensitive data, applications, and backups. Misconfigured or unprotected cloud systems could expose sensitive information publicly, leading to unauthorized access or data leaks. Additionally, cloud platforms are often targeted by attackers aiming to exploit storage misconfigurations or weak access controls. A compromised cloud environment could result in the theft of customer data, disruption of services, and loss of critical backups, crippling business operations. Such incidents could also violate regulatory requirements, exposing DGT to fines and legal consequences. (*Empowering and Securing Banking and Financial Organizations*, 2023)

14. Employee Workstations

Workstations are used by employees to access critical systems, handle sensitive data, and communicate with clients. They are often targeted by attackers through phishing, malware, or social engineering, as workstations can act as an entry point to DGT's internal network. A compromised workstation could allow attackers to exfiltrate customer data, steal login credentials, or spread malware across the organization. Additionally, human error or negligence on workstations, such as clicking on malicious links or downloading unauthorized software, could lead to significant security breaches. Protecting workstations is essential to maintain the confidentiality, integrity, and availability of DGT's data and systems. (Clifton, 2024)

15. Automated Teller Machines

Automated Teller Machines (ATMs) are a crucial component of digital banking services that enable customers to perform essential financial transactions such as cash withdrawals, deposits, balance inquiries, and fund transfers while maintaining efficiency, convenience and accessibility. As ATMS are primary targets for attackers to install skimmers, malware and unauthorised malicious tools, it is important for DGT to secure and enforce this asset, so as to provide ease of access, security to their customers and avoid financial losses, legal liabilities, and damage to an organisation's reputation. (Koch, 2024)

16. Customer Records and Document archives

Customer records and document archives store sensitive personal and financial data about clients. These may include Personal Identifiable Information (PII), Legal documents and archived data. Should these documents be leaked, stolen or even manipulated, the bank could expect to face losses in the form of financial losses due to breaches in data protection, fraud and even compensation fees. Customers may also lose trust in the organisation due to sloppy handling of sensitive information which leads to reputational damage.

17. HQ External Router

The external router is how the DGT headquarters connects to the internet, serving as the primary gateway for network traffic. It plays a critical role in managing incoming and outgoing data, enforcing security policies, and preventing unauthorized access to the internal network. If compromised, attackers could intercept sensitive communications, conduct man-in-the-middle attacks, or disrupt banking services through denial-of-service (DoS) attacks. Ensuring the router is properly configured, regularly updated, and protected with firewall rules is crucial to safeguarding DGT's network infrastructure and maintaining secure online banking operations.

Asset Inventory

Asset	Confidentiality	Integrity	Availability
Customer Information	- There is a risk of identity theft and fraud if personal data is leaked. - Threat of compliance risks (like GDPR penalties).	- Data alteration can result in incorrect customer records, which will lead to service issues and legal liability. - Fraudulent transactions can happen if information is tampered with.	- Customer support is impacted if certain data is unavailable. - Service disruptions can happen if identity verification systems rely on customer data.
Financial Transaction Data	- Unauthorized access to financial transaction data can lead to fraudulent transactions, which will result in financial loss for customers. - High regulatory scrutiny and potential fines for data breaches.	- Any unauthorized changes can lead to financial discrepancies and errors in transaction records. - Undetected tampering can facilitate fraud.	- Loss of transaction data availability could temporarily halt financial operations, impact customer trust, and disrupt business.
Third-party and Vendor Information	- Leakage of vendor contracts and access credentials could lead to unauthorised system access. - There may be potential competitive disadvantage(s) if agreements or pricing are exposed.	- Altered contract terms or service levels can lead to service disruptions or overbilling. - Integrity issues can lead to compliance and audit challenges.	- Unavailable vendor information can disrupt service continuity. - Delays in vendor communication can additionally lead to operational inefficiencies.

Employee Information	● Identity theft and privacy risks if personal employee data is exposed. ● There will be an impact on employee trust and morale.	● Changes to payroll, benefits, or tax information can lead to financial or legal consequences for employees and the organization.	● HR and payroll disruptions if employee data is inaccessible. ● Chance of potential delays in employee services and support.
Intellectual Property and Trade Secrets	● Loss of proprietary information or trade secrets can result in a competitive disadvantage. ● Risk of misuse by competitors or threat actors.	● Tampering with proprietary algorithms or software could lead to incorrect financial analyses or risk assessments, impacting decision-making and services.	● Loss of access to IP could hinder innovation and disrupt ongoing projects, affecting business growth and development.
Customer Behavioural and Analytics Data	● Leaking of customer behaviour patterns could lead to targeted phishing or fraud schemes, severely impacting customer safety and trust. ● Competitors could misuse this data to gain an unfair advantage over DGT.	● Tampering with analytics data could lead to incorrect business decisions, such as flawed marketing strategies or inaccurate risk assessments. ● Altered data may also reduce the institution's ability to predict customer needs.	● Lack of access to behavioural analytics during critical periods could limit DGT's ability to adapt to market trends or meet customer expectations. ● Operational agility would be severely reduced.

Unreleased Financial Products or Services	● Leaking of new product plans could give competitors the opportunity to copy or pre-emptively launch similar services, harming DGT’s competitive edge. ● Customers may lose confidence in the company’s confidentiality standards.	● Alterations to unreleased product details could disrupt launch schedules, confuse stakeholders, or mislead development teams. ● Incorrect versions of product information might be distributed internally.	● The unavailability of development or product launch data could cause delays in deployment, impacting revenue and customer trust. ● Future projects may be delayed or derailed entirely.
Online Banking Information	● Unauthorised access to online banking data, such as PayNow or FAST transactions, could lead to identity theft and financial fraud. ● Sensitive user credentials and transaction records must remain private to maintain customer trust and comply with regulations.	● Data tampering could result in transactions not by the user or errors in financial processing. ● Altered records could lead to disputes, financial discrepancies, and legal complications.	● Unavailability of online banking services, especially real-time payment platforms like PayNow, could disrupt customers’ ability to perform transactions, impacting trust and satisfaction.
CRM Server Information	● A breach could expose customer data, including personal details, financial histories, and communication logs, leading to identity theft or misuse. - Confidentiality is critical to uphold customer trust and regulatory compliance.	● Unauthorised changes to CRM data could lead to misinformation during customer interactions. ● Corrupted data could impair the quality of service provided to clients.	● Loss of access to CRM systems would disrupt customer service, leading to frustration, inefficiency, and erosion of trust in DGT’s ability to maintain seamless operations.

External Firewall	● A misconfigured or breached external firewall can allow unauthorized access to DGT’s online banking systems, exposing customer account details, financial transactions, and sensitive business data. ● Inadequate firewall rules may allow unfiltered external traffic, leading to data exfiltration through techniques like covert channels, botnets, or remote access trojans (RATs).	● **A**ttackers may exploit firewall vulnerabilities to insert malicious traffic, leading to data corruption, fraudulent transactions, or DNS poisoning attacks. ● Weak security policies in firewall rules could allow attackers to inject or manipulate traffic, altering customer requests (e.g., fund transfers, login credentials).	● **D**istributed Denial-of-Service (DDoS) attacks can overwhelm the firewall, disrupting online banking operations and preventing legitimate users from accessing services. ● Failure or misconfiguration in the firewall may cause network bottlenecks, affecting banking servers, CRM systems, and remote branch connections.
Internal Firewall	● If the internal firewall is bypassed or compromised, attackers can move laterally within the internal network, gaining access to back-end banking servers, administrative consoles, and confidential financial data. ● Poorly enforced segmentation between internal systems (e.g., CRM, transaction processing, and authentication servers) may expose highly privileged data to unauthorized users	● Compromised internal firewall rules could allow malicious packets to spread across internal systems, leading to data integrity violations, tampered transaction records, and unauthorized database modifications. ● Attackers may leverage internal misconfigurations to inject malicious scripts or commands, disrupting automated banking workflows.	● Failure of internal firewall segmentation could allow malware or ransomware to propagate unchecked, leading to bank-wide outages. ● Improper firewall rules might cause disruptions in branch-to-HQ communications, impacting transaction approvals, CRM functionality, and authentication systems.

	or malicious insiders.		
Virtual Private Networks	● Unauthorized access to DGT’s VPN can expose sensitive internal banking communications and customer data. ● Leaked VPN credentials can compromise secure connections within DGT's network. Mismanaged VPN configurations can allow attackers to intercept traffic, violating confidentiality.	● Misconfigured or tampered VPN settings can redirect or block traffic, causing security breaches and operational issues for DGT's online banking services. ● Corrupted VPN software could disrupt the integrity of encrypted banking communications.	● VPN downtime could prevent secure communication between DGT’s remote employees, leading to interruptions in critical banking operations. ● Service unavailability may halt business continuity for online transactions.
Cloud Infrastructure	● Data breaches in DGT’s cloud environment could expose sensitive customer financial data, including transaction logs. ● Improper access control could lead to data leaks and non-compliance with financial regulations.	● Alterations to DGT’s cloud configurations could cause operational errors or incorrect financial computations. ● Fraudulent activities may arise if customer data stored in the cloud is tampered with.	● Downtime in DGT’s cloud services could disrupt online banking functionalities, including account management and transaction processing. ● Unavailability may impact disaster recovery, backups, and real-time operations for

			critical banking services.
Employee Workstations	● Malware or phishing attacks targeting DGT's employee devices could lead to unauthorized access and sensitive data exfiltration. ● Unsecured workstations may inadvertently expose critical customer or banking information.	● Altered system files or unauthorized changes on DGT employee workstations could introduce security vulnerabilities or lead to incorrect data processing. ● Fraudulent banking operations might occur if employee credentials or files are tampered with.	● Compromised or malfunctioning employee workstations could halt critical banking tasks, such as customer support or backend system operations. ● Downtime significantly impacts overall productivity and DGT's business continuity.
Automated Teller Machines (ATMS)	● Unauthorized access or tampering with DGT ATMs could result in card skimming or the exposure of customer account details. ● Compromised ATM configuration files could lead to security breaches.	● Tampered ATM software could result in incorrect or fraudulent transactions, impacting DGT's financial integrity. ● Systematic errors caused by altered software may create legal and reputational risks for DGT.	● Unavailability of ATMs would directly disrupt customer transactions, impacting withdrawals, deposits, and other banking services. ● Prolonged downtime could harm customer trust and DGT's

			reputation in financial services.
Customer Records and Document Archives	● Unauthorized access to DGT’s customer records and archives could result in identity theft and the exposure of sensitive customer information. ● Data breaches could lead to regulatory fines and penalties for DGT.	● Alterations to DGT’s customer records or archives could result in inaccurate transaction records or compliance issues. ● Fraudulent or corrupted data could lead to reputational damage and loss of customer trust.	● Unavailable archives could disrupt DGT’s customer verification processes and delay services, such as dispute resolution or loan approvals. ● Service interruptions might arise if archived data is critical for audits or regulatory reporting.

Asset classification

Information Classification Levels	
Classification	**Description**
Public	Information that can be freely shared with the public without any risk. This data does not require security controls.
Internal	Information intended for internal use only. Its disclosure outside the organization is not permitted unless authorized, but it poses minimal risk.
Restricted	Sensitive information that could cause harm if exposed. Access should be limited to authorized individuals, and security controls must be in place.
Confidential	Critical information that, if disclosed, could cause severe harm to the organization or individuals. Requires strict access controls and encryption.

Table 3.1, Asset Classification Levels

Table 3.1 defines the different classifications. Using this table, we can classify the information assets

Information asset	Classification	Reason
Customer information	Restricted	Contains sensitive personal and financial details that could lead to identity theft or financial loss if exposed.
Financial Transaction Data	Confidential	Involves critical financial data that needs protection against fraud, theft, or unauthorized access.
Third-party and Vendor Information	Restricted	Contains contracts, agreements, and sensitive business data requiring protection for trust and legal compliance.
Employee information	Restricted	Personal and employment data that require privacy and legal compliance.

Intellectual Property and Trade Secrets	Confidential	Includes proprietary information vital for competitive advantage, needing protection from industrial espionage.
Incident Response and Security Policies	Confidential	Contains detailed procedures and strategies for handling security incidents. Exposure could aid attackers in targeting vulnerabilities or evading detection.
Regulatory and Compliance Data	Restricted	Includes sensitive information about compliance with financial and data protection laws. Loss or exposure could lead to legal penalties and regulatory scrutiny.
Customer Behavioural and Analytics Data	Restricted	Involves insights into customer behaviour, transaction patterns, and analytics used for targeted services. Exposure could result in privacy violations and breaches.
Unreleased Financial Products or Services	Confidential	Information on products or services that are under development but not yet launched. Exposure could lead to a loss of competitive advantage or market disruption.
External Firewall	Restricted	First line of defense; compromise could lead to unauthorized access.
Internal Firewall	Confidential	Protects internal systems; breach could expose critical security configurations.
CRM Server Information	Confidential	Stores critical business and customer data requiring strict access control.

Customer Records and Document Archives	Confidential	Contains sensitive personal and financial information that must be encrypted and secured.
Automated Teller Machines	Confidential	Handles financial transactions; compromise could lead to monetary theft or fraud.
Employee Workstations	Internal	These are used for business operations; exposure poses minimal but manageable risk.
Cloud Infrastructure	Restricted	Hosts multiple services; a breach could impact business operations.
VPN	Restricted	Provides secure remote access; compromise could expose internal systems.
Online Banking Information	Confidential	Critical financial data; breach could lead to fraud and severe financial loss.
Unreleased Financial Products or Services	Confidential	Proprietary business information; exposure could lead to competitive disadvantages.

Weighted Factor Analysis Worksheet

The criteria considers the following:

- **Impact on Revenue (30%)**: A breach or incident affecting the revenue directly impacts DGT Bank's profitability and business continuity. This could occur through penalties, lost customers, fraud, or operational disruptions. This is why it is assigned the greatest weightage among all the different impacts.
- **Impact on Public Image (25%):** The reputation of our bank is vital to maintaining customer trust and market competitiveness. A security incident could result in negative press, loss of customer confidence, and a damaged reputation, potentially causing long-term financial impacts
- **Impact on Operation (20%):** Our bank must be able to provide efficient operation to ensure timely and reliable financial services. If a breach occurs or if key systems are disrupted, the ability to serve customers and process transactions is impacted. However, it has the least priority given that they usually can be resolved the quickest compared to other impacts.
- **Impact on Customer Trust (25%):** Customer trust is essential for the long-term success of our bank because our customers must trust the bank to handle their sensitive information securely. A data breach or security failure could damage that trust, leading to customer attrition and a damaged reputation.

The following table presents the weighted factor analysis worksheet. This allows us to identify and prioritise key assets, which will deal serious damage to the company should something happen to the asset.

To calculate the importance or weightage of each asset, we use the formula:

Weighted Score = (**Impact to Revenue**×30) + (**Impact to Public Imag**e×25) + (**Impact to Operation**×20) + (**Impact to Customer** Trust×25)

(0 being the lowest and 1 being the highest)

Information asset	**Impact to revenue**	**Impact on public image**	**Impact to operation**	**Impact to customer trust**	**Weighted score**
Criterion weight (1-100)	30	25	20	25	**100**
Customer information	0.8	1	0.7	1	**88**
Financial Transaction Data	0.9	0.9	0.7	1	**88.5**
Third-party and Vendor Information	0.7	0.8	0.7	0.7	**72.5**
Employee information	0.8	0.7	0.5	0.6	**66.5**
Intellectual Property and Trade Secrets	0.9	0.8	0.7	0.7	**78.5**
Regulatory and Compliance Data	0.7	0.7	0.7	0.7	**70**
Customer Behavioural and Analytics Data	0.9	0.9	0.8	0.9	**87.5**
Unreleased Financial Products or Services	0.9	0.7	0.9	0.7	**80**
Firewalls (HQ and Branch firewalls)	0.8	0.9	0.7	0.9	**86**
VPN Cloud	0.9	0.8	1	0.9	**89.5**
CRM Server	0.9	0.8	0.9	0.9	**87.5**
Online Banking System Server	1.0	1.0	1.0	1.0	**100**

CRM Clients (at branches)	0.7	0.6	0.7	0.6	**67.5**

Justification

1. **Customer information**
    a. ***Impact to revenue (0.8)***: Compromise regarding customer information can indirectly lead to losses in revenue because customers may avoid and stop using our bank. The banking act protects confidentiality of customers data and results in severe penalties in the event of non compliance.
    b. ***Impact to public image(1)***: A leak in customer information is a serious issue and the reputation of the bank will be severely impacted. The damage in reputation will also likely last a long time.
    c. ***Impact to operation (0.7)***: During a breach, some operations may be indirectly affected. Such operations may include customer management services.
    d. ***Impact to customer trust(1)***: A breach in customer information is a major issue since private information such as their NRIC number may be leaked. Customers can no longer trust us, which may lead to loss of business

2. **Financial transaction data**
    a. ***Impact to revenue (0.9)***: A leak in financial transaction data can indirectly lead to losses in revenue because customers may avoid and stop using our bank. Several laws such as the banking act and MAS notice 644 protects confidentiality of financial transaction data and results in severe penalties in the event of non compliance.
    b. ***Impact to public image(0.9)***: Although the reputation of the bank will be severely damaged, the damage in reputation will not be as severe as a leak in customer information.
    c. ***Impact to operation (0.7)***: Operations will likely be indirectly affected while trying to resolve the issue
    d. ***Impact to customer trust(1)***: A breach in customer information is a major issue since private information such as their bank account number may be leaked. Customers can no longer trust us, which may lead to loss of business

3. **Third-party and Vendor Information**
    a. ***Impact to revenue (0.7)***: Several laws such as the banking act and Outsourcing Guidelines by the Monetary Authority of Singapore(MAS) protects confidentiality of financial transaction data and results in severe penalties in the event of non compliance. The likelihood of customers avoiding the bank is lower than if more personal data was leaked.
    b. ***Impact to public image(0.8)***: The reputation of the bank will likely be damaged given that information was able to be breached. The reputation damage would not be as great as if personal data was leaked.

c. ***Impact to operation (0.7)***: Operations will likely be indirectly affected while trying to resolve the issue

d. ***Impact to customer trust(0.7)***: While customer trust will reduce, a breach in third party and vendor information that does not directly concern them and will not drop too much

4. **Employee information**
    a. ***Impact to revenue (0.8)***: Several laws such as the Personal Data Protection Act and Employment Act protects employee information. Significant penalties will be applied in the event of non compliance. There is also the risk of employee lawsuits in the event of a data breach.
    b. ***Impact to public image(0.7)***: A data breach involving employee information will be damaging but not as damaging as customer information being involved in the breach.
    c. ***Impact to operation (0.5)***: Since the issue is internal, the impact to operations for the customer will not be impacted too much.
    d. ***Impact to customer trust(0.6)***: Customer trust will not reduce as much as compared to a breach in customer information that directly concerns them

5. **Intellectual Property and Trade Secrets**
    a. ***Impact to revenue (0.9)***: Intellectual property and trade secrets being exposed to our competitors will cause us to lose our advantage over our competitors. The amount of customers we have will likely reduce or remain stagnant, causing our revenue to be negatively impacted
    b. ***Impact to public image(0.8)***: A breach in intellectual property and trade secrets will suggest weak data protection controls in place in the bank. Our reputation will be damaged, but not to the extent as if customer data was breached.
    c. ***Impact to operation (0.7)***: This can lead to damages in long term operations, since trade secrets were breached and would require coming up with new and innovative approaches.
    d. ***Impact to customer trust(0.7)***: Customer trust will decrease because if the bank’s property can be breached, they would believe their personal data could too. However, it does not directly affect them so it will not reduce too much.

6. **Regulatory and Compliance Data**
    a. ***Impact to revenue (0.7)***: If the data is tampered or deleted during an incident, we will be subject to multiple fines for breaking several laws. This includes workplace safety and health act and companies act , which comes with a fine of $500 000 and $5000 respectively.
    b. ***Impact on public image (0.7)***: A data breach involving regulatory and compliance data will be damaging but not as damaging as customer information being involved in the breach.
    c. ***Impact to operation (0.7)***: Operations may not be directly affected, but it will be slowed since the data will have to be rechecked or redone.

   d. ***Impact to customer trust (0.7)***: Customer trust will not reduce as much as compared to a breach in customer information. However, it will cause us to be less trustworthy as a result of this attack.

7. **Customer Behavioural and Analytics Data**
   a. ***Impact to revenue (0.9)***: This data allows us to conduct personalised marketing and product recommendations. A security incident can impact our ability to carry out these activities, thereby losing revenue. Customers may also avoid using our bank since their privacy can no longer be guaranteed.
   b. ***Impact on public image (0.9)***: Behavioural and analytics data are considered very personal information and will cause our public reputation to be severely impacted.
   c. ***Impact to operation (0.8)***: If the data is the subject of an attack, marketing campaigns and customer analysis processes will have to be placed on a temporary halt, disrupting our operations.
   d. ***Impact to customer trust (0.9)***: Customer trust will likely significantly decrease since the data can be seen as personal data. Customers may also avoid us since such data can be used for spear phishing attacks which are highly effective.

8. **Unreleased Financial Products or Services**
   a. ***Impact to revenue (0.9)***: A leak of our unreleased products and services will severely damage our competitive advantage. Our competitors will be able to create similar products and services, causing us to attract less customers and
   b. ***Impact on public image (0.7)***: A data breach concerning our unreleased products and services will raise questions about how good our security is, which will cause our security reputation to drop
   c. ***Impact to operation (0.9)***: Leakage of the unreleased products or services will set us behind schedule since we have to come up with new plans, marketing and launch dates will have to be pushed back
   d. ***Impact to customer trust (0.7)***: Customer trust in our bank will drop since a data breach has successfully occurred. Customers may also switch to other banks if they release similar products with more enticing features.

9. **Firewalls (HQ and Branch firewalls)**
   a. ***Impact to revenue (0.8)***: Indirect impacts on our revenue will occur if our firewalls are attacked. Firewalls are our first line of defence, and if compromised, customers may leave. However, softwares such as antiviruses will likely protect key servers.
   b. ***Impact on public image (0.9)***: If customer information are exposed as a result of an attack on the firewall, the reputation of the bank will be tarnished
   c. ***Impact to operation (0.7)***: Firewall issues can disrupt communications between the branches and HQ, which will disrupt our operations.
   d. ***Impact to customer trust (0.9)***: Firewall issues or compromise can lead to private and sensitive customer information to be exposed, causing our customers

to lose trust in our security system.

10. VPN Cloud

a. ***Impact to revenue (0.9)***: The impact on revenue is high due to the VPN cloud's role. It is the centre point of our communications, so if the VPN cloud is the subject of an attack, there will be no access to revenue generating services at all.
b. ***Impact on public image (0.8)***: If the VPN cloud has been compromised, attackers can use it to steal data since all communications go through it. If the cloud does not work properly, services will be disrupted. This will all cause the reputation of the bank to drop significantly.
c. ***Impact to operation (1)***: The VPN cloud is the key component of our operations. Without it, key services and basic communications between HQ and the branches will not be able to occur.
d. ***Impact to customer trust (0.9)***: A VPN failure can cause disruptions to daily activities for our customers. Accessing online banking services will be disrupted, causing our customers to lose trust in our bank's reliability.

11. CRM Server

a. ***Impact to revenue (0.9)***: The CRM server performs analytics on customer data for the frontline service personnel to advise on customer's credit limit and financial planning. If the server is down, this service will be delayed, which can lead to potential revenue loss.
b. ***Impact on public image (0.8)***: If attackers attack and gain access to the CRM server, sensitive customer data may be compromised. Sensitive information being leaked will cause the bank's reputation to be tarnished.
c. ***Impact to operation (0.9)***: If the CRM server is down, operations related to customer relations will be down.
d. ***Impact to customer trust (0.9)***: In the event an attack on the CRM server causes their data to be leaked, customers will no longer trust us.

12. Online Banking System Server

a. ***Impact to revenue (1)***: Delays in online banking services will directly cause revenue loss. Information found in this server often contains highly confidential information, so a data breach of this server will cause customers to leave thus causing revenue loss.

b. ***Impact on public image (1)***: A compromise of the server is a serious cybersecurity incident and will cause our reputation to drop.

c. ***Impact to operation (1)***: If the server is down, key banking operations such as payment will be down. This has the greatest impact on our operations since the activities are often time sensitive.

d. ***Impact to customer trust (1)***: Without reliable service or guaranteed security and privacy, customers will no longer trust us.

13. CRM Clients (at branches)

a. ***Impact to revenue (0.7)***: CRM services generate revenue for the bank. If the CRM clients at the branches do not work, we will lose revenue during that period. However, it is unlikely all branches will encounter issues at the same time.

b. ***Impact on public image (0.6)***: Disrupted services will cause the bank's reputation to drop but it is not as severe as data breaches.

c. ***Impact to operation (0.7)***: Operations will be affected at the branches where the CRM clients are down.

d. ***Impact to customer trust (0.7)***: Customers will not be able to trust our bank if CRM clients are affected as the services we provide will be deemed as unreliable.

Threat Identification

Criteria to prioritise threats:

- Which threats present a danger to assets?
- Which threats represent the most danger to information?
- How much will it cost to recover from attacks?
- Which threat requires the greatest expenditure to prevent?

With support from evidence, in no particular order, the **top 10** threats for DGT Bank:

- **Threat 1:** Advanced persistent threats (APT)
- **Threat 2:** Ransomware and malware
- **Threat 3:** Insider threat
- **Threat 4:** Third-party vendor compromise
- **Threat 5:** Data breach
- **Threat 6:** Privilege escalation
- **Threat 7:** Cloud Compromise
- **Threat 8:** Man-in-the-middle attacks
- **Threat 9:** Social engineering
- **Threat 10:** Denial of Service attacks

Justification

Before we begin, here is a summary of the **top 10 identified threats**, in a table form for easy reference.

ID	Threat	Description	Key Statistics / Example	Impact
T1	Advanced Persistent Threat (APT)	Long-term campaigns where attackers establish presence in a network to steal sensitive data. Commonly use Active Directory for lateral movement.	80% of attacks involve Active Directory; IBM X-Force observed APT-style attacks with Mimikatz to access POS systems.	Data exfiltration, extended presence in networks, and potential operational impact.
T2	Ransomware & Malware	Malicious software that disrupts operations, encrypts data, and demands ransom. Includes backdoors, cryptominers, infostealers, worms, and web shells.	Malware was the most common action in 43% of incidents; ransomware accounted for 20% of reported cases in 2023.	Financial loss, operational downtime, and data theft.
T3	Insider Threat	Threats posed by employees or contractors, either intentionally or accidentally. Recent tactics include AI-generated résumés for insider placement.	2024 report noted the use of AI to create insider profiles to infiltrate companies.	Data leakage, intellectual property theft, and sabotage.
T4	Third-Party Vendor Compromise	Attackers exploit vulnerabilities in third-party services to gain access. Supply chain compromises are a common tactic.	Crowdstrike 2024: Compromise of Falcon Sensor affected 8.5M systems, costing $10B.	Widespread disruption and financial loss due to compromised services.
T5	Data Breach	Unauthorized access to sensitive data, often through large-scale breaches or AI vulnerabilities.	Over 80% of organizations experience multiple data breaches; CaaS	Data exposure, identity theft, and regulatory penalties.

			economy simplifies fraud schemes.	
T6	Privilege Escalation	Attackers gain elevated privileges to bypass security controls, often targeting cloud environments or exploiting Active Directory vulnerabilities.	Scattered Spiders obtained cloud admin privileges; 4.18% of attacks involved privilege escalation in 2024.	Full system control, data exfiltration, and lateral movement within networks.
T7	Cloud Compromise	Adversaries target cloud environments to exploit unique cloud workflows.	Cloud intrusions increased by 75% from 2022 to 2023; SCATTERED SPIDER accounted for 29% of cloud-conscious attacks.	Data loss, service disruption, and potential geopolitical impact.
T8	Man-in-the-Middle Attacks	Adversaries intercept communications to steal credentials, including MFA codes.	2023: IBM X-Force observed multiple adversary-in-the-middle (AitM) attacks, bypassing MFA using phishing and reverse-proxy techniques.	Credential theft, privilege escalation, and identity compromise.
T9	Social Engineering	Psychological manipulation to trick users into revealing confidential information. Often bypasses security measures like MFA.	Increased use of legitimate tools makes it hard to detect breaches; AI-generated attacks are also on the rise.	Unauthorized access, financial loss, and data breaches.
T10	DDoS Attacks	Attackers flood systems with traffic to overwhelm services, causing downtime and disruption.	DDoS attacks surged by 200% in 2023; IoT botnets like Mirai are commonly used to execute these attacks.	Service disruption, financial loss, and reputational damage.

Threat 1: Advanced persistent threats (APT)

Advanced persistent threats are attack campaigns in which an intruder, or team of intruders, establishes an illicit, long-term presence on a network to obtain and exfiltrate highly sensitive data. IBM X-Force Threat Intelligence observed financially motivated actors adopting advanced persistent threat (APT)-style attacks leveraging Mimikatz and Active Directory to move throughout the network to gain access to the POS systems.[1][2] Till today, Active Directory remains in use at over 75,000 companies globally,[3] and a 2021 industry report states that 80% of attacks use Active Directory to perform lateral movement and privilege escalations.[4] APT remains a critical point of interest when considering our areas of security measures.

Threat 2: Ransomware and malware

While ransomware makes up a relatively small percentage of overall malware detections, it still packs the biggest punch in terms of impact. Additionally, according to IBM X-Force Incident Response data, deployment of malware was the most common action threat actors took on victim networks, occurring in 43% of all reported incidents. Of the total incidents, 20% were ransomware cases. Backdoors and crypto miners were discovered in 6% and 5% of cases, respectively. The remaining malware incidents included infostealers, loaders, bots, worms, web shells and downloaders. As mentioned, extortion-based attacks remained one of the driving forces of cybercrime in 2023 with threat actors leveraging various attack types to deliver on their extortion objectives. more than doubled in 2023, and the percentage of incidents that were extortion-based increased from 21% in 2022 to 24% in 2023.[5]

Threat 3: Insider threat

Insider threats will always remain a critical flaw in computer security, primarily due to the unpredictability of human nature. In 2024, Cloudstrike observed how adversaries achieved initial access, and amongst the most common methods lies Insider Threats, together with accidental credential leakage, brute-force attacks, phishing/social engineering, credential stealers, access brokers and insecure self-service password-reset services. In addition, according to Microsoft Digital Defence Report 2024, threat actors could be using AI to scrape keywords and qualifications from job listings to create hundreds or thousands of various “perfect” candidates for a job position, even involving the use of steganography techniques to hidden information to increase their chances of passing automated screening tools, with a goal to place insiders within an organisation to steal treat secrets, intelligence, or otherwise sensitive information. Alternatively, threat actors may instead choose to create a swarm of AI-generated underqualified résumés together with a few “ideal” candidates to break screening process.[6]

Threat 4: Third-party vendor compromise

As observed during the Crowdstrike outage in 2024, the reliance on Cloudstrike, a third-party platform that provides threat intelligence, endpoint security, and cyber attack response services for its clients, caused widespread issues with Windows computers, crashing about 8.5 million systems affecting many critical industries and governments, including airlines, banks, hospitals, and stock markets, and was estimated to have caused at least $10 billion in financial damage, all occurred due to a faulty update to its Falcon Sensor security software. This highlighted not only the importance of having robust crisis management plans but also the risks of relying too much on a single system or provider. In our case, according to Cloudstrike’s own Global Threat Report of 2024, targeted intrusion actors exploited trusted relationships between companies and their third-party providers to gain initial access, taking advantage of these vendor-client relationships to deploy malicious payloads via compromising the software supply chain with trusted software to spread malicious tooling or by leveraging access to vendors supplying IT services. are motivated by the potential return on investment (ROI): One compromised organisation can lead to hundreds or thousands of follow-on targets. These stealthy attacks can also more effectively provide an opportunity for attackers seeking to exploit a hardened end target.[6]

Threat 5: Data breach

In an ever-evolving cyber threat landscape, traditional methods such as exploiting large-scale data breaches remain prevalent, enabling threat actors to bypass security measures and access extensive personal data. According to Microsoft Threat Report 2024, the growth of the Containers as a Service (CaaS) economy has also greatly simplified the execution of complex fraud schemes by providing ready access to stolen data and fraudulent tools needed. With the exponential growth of generative AI, emerging AI apps that are deployed on ungoverned data assets could result in data oversharing or leakage as threat actors could exploit specially crafted prompts to gain access to sensitive data. Studies have shown that over 80% of organisations experience multiple data breaches over time, so getting ahead of the risks is critical to business operations, but at the same time, it is difficult to intentionally protect sensitive data from AI-related security risks given that many organisations do not fully know where or what their sensitive data is. This makes it all the more important to focus on, especially when considering the resulting consequence if such an event were to actually occur.[7]

Threat 6: Privilege escalation

Adversaries’ preference for identity-based techniques is evident in their cloud-focused attacks, as observed above.

In one of the attacks carried out by Scattered Spiders, during the intrusion of a North American Software Company, Scattered Spiders managed to obtained elevated privileges by attaching a new administrator policy to an existing cloud user, to which they added a new access key (Kurtz & CrowdStrike, 2024, p. 18) [6].

If we extrapolate our observations and fit them to the observations of cloud and identity focused activities categorized by the MITRE ATT&CK® enterprise tactics *(Initial Access, Persistence,* ***Privilege Escalation****, Credential Access, Lateral Movement, Exfiltration and Impact)*, we can observe a striking resemblance to one of the Privilege Escalation techniques T1484. Just by itself, this is an incredibly impactful threat if left unaccounted for, as any instance where an adversary would be able to gain elevated privileges in our network would mean all controls from there on would be obsolete, as they would be able to be overwritten. Therefore, this is an incredibly dangerous threat if a related technique were to be exercised by a sufficiently capable adversary. Referring back to the threat report conducted by Cloudstrike, adversaries who managed to obtain elevated privileges by gaining access to additional identities from stored credentials, social engineering campaigns or insecure password-reset portals were also observed as well, in addition to modifying policies or adding identities to privileged groups or roles as mentioned above.

Taking a look at the distribution of tactics used by adversaries to achieve their objectives in 2024, we can observe a non-insignificant amount of privilege escalation attempts at around 4.18%. However, in a surprising turn of events, Elastic observed a 2% reduction in detections related to privilege escalation compared to 2023 -- the growing threat of information stealers and widespread distribution of stolen credentials may have reduced the need for privilege escalation.

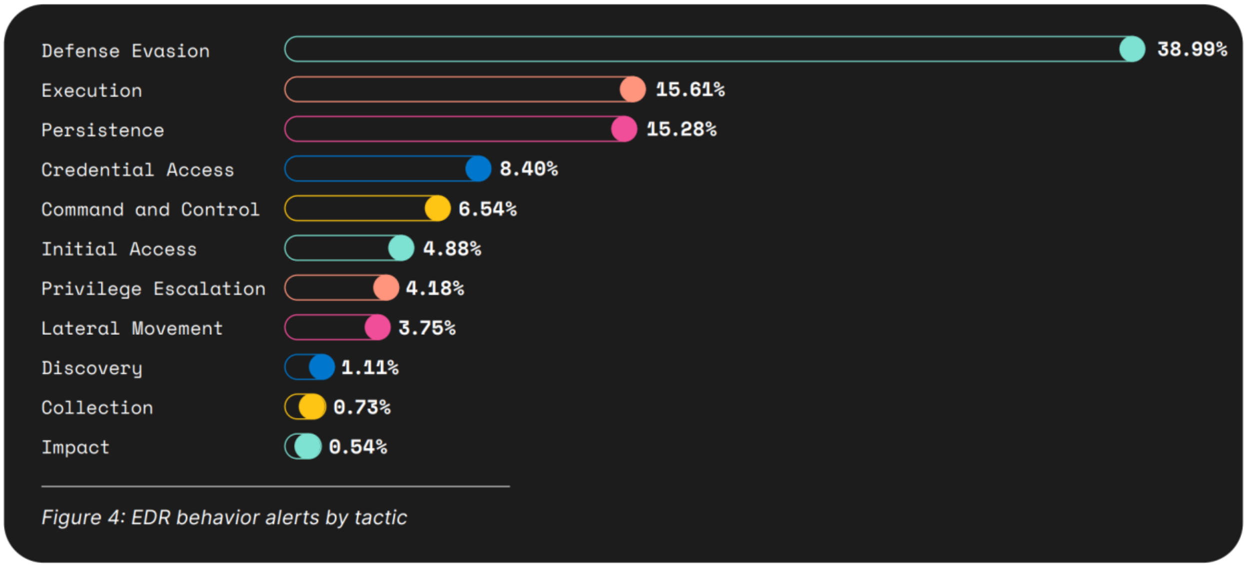


Figure 4: EDR behavior alerts by tactic

Figure 1.

Elastic Security Labs. (2024). *2024 Elastic Global Threat Report*.

Microsoft has also observed the use of BEC lateral phishing to achieve lateral movement in conjunction with privilege escalation. “After compromising an account, attackers would aim to move laterally within the organization, targeting multiple users to either gain access to high-privilege accounts or trick users into paying fake invoices. This is achieved by sending phishing emails to other users within the organization.” [7]

Similarly, IBM X-Force also observed attackers focusing on SPNs associated with service accounts, as these accounts often hold higher permissions, facilitating broader access to data and systems. “Financially motivated attackers in 2023 also targeted Active Directory Certificate Services (AD CS) for privilege escalation, exploiting CVE-2022– 26923 to potentially elevate their privileges to domain administrator. Although Microsoft patched this vulnerability in update KB5014754, successful attacks can still occur depending on key distribution center (KDC) configurations, underscoring the importance of vigilant patch management and secure service settings.”

Threat 7: Cloud Compromise

As predicted by Crowdstrike, an increase in cloud environment intrusions by 75% from 2022 to 2023 has been observed, with cloud-conscious cases increasing by 110% and cloud-agnostic cases increasing by 60%.

Cloud-conscious refers to adversaries that are aware of the ability to compromise cloud workflows and utilise this knowledge to abuse features unique to cloud for their own goals.

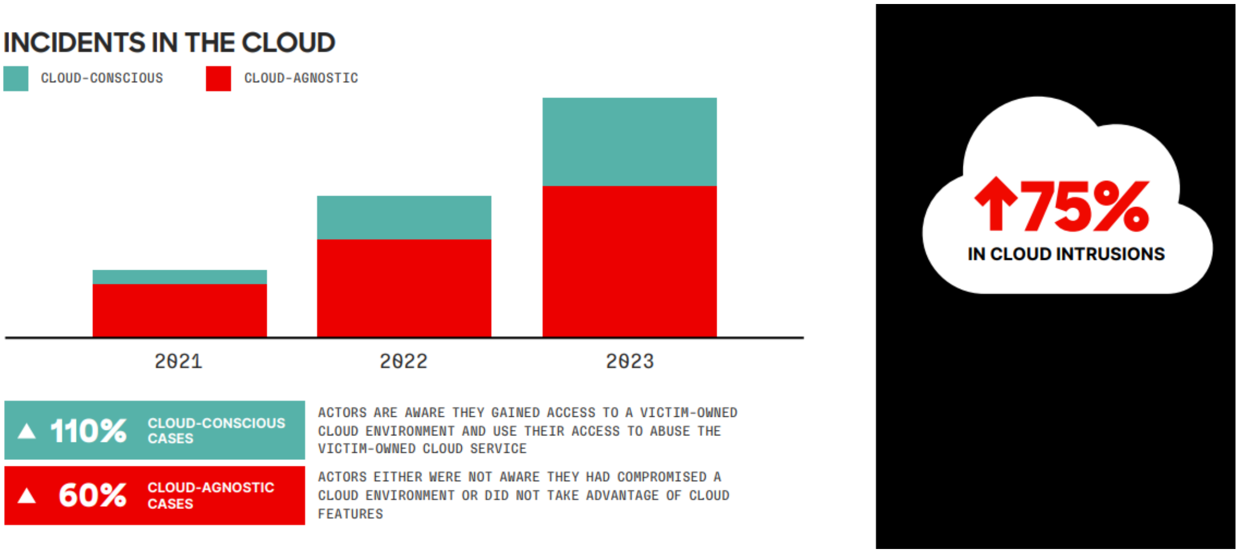


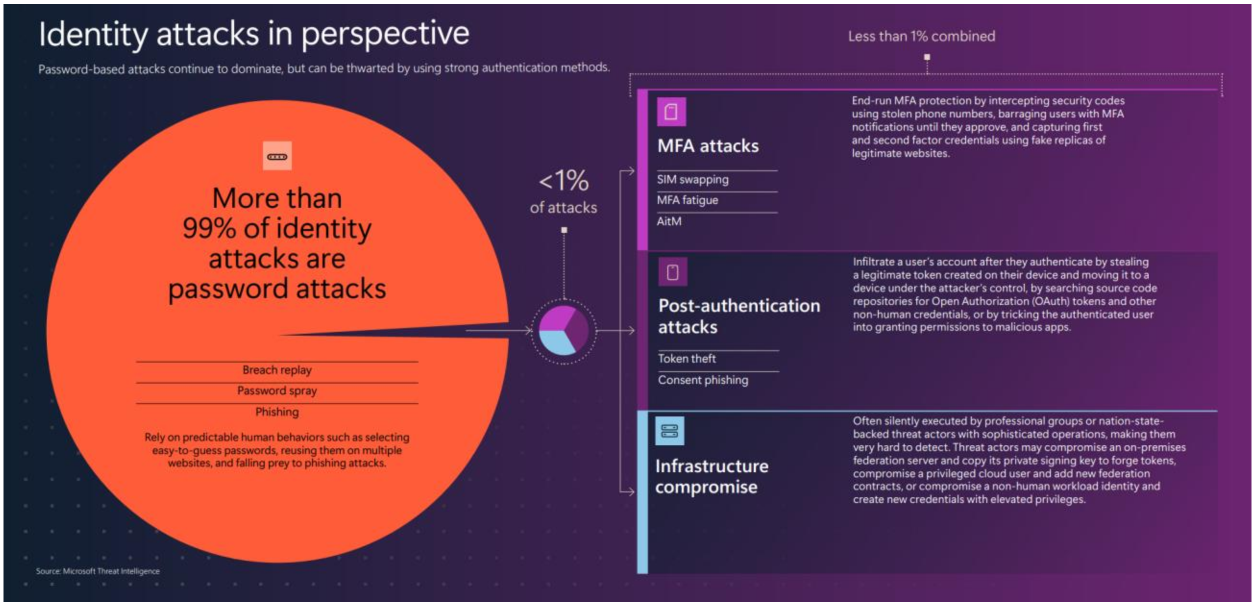
Figure 2.

Kurtz & CrowdStrike (2024, p. 17, *Fig. 2*)

One of the most notable adversaries, SCATTERED SPIDER predominantly drove cloud-conscious activities increases throughout 2023, accounting for 29% of total cases. A brief background check on SCATTERED SPIDER (also known as **UNC3944**), a hacker group primarily made up of operatives based in UK and US, gained their notoriety for their involvement in the hacking and extortion of Caesars Entertainment and MGM Resorts International, two of the largest casino and gambling companies in the United States. However, Scattered Spider has also targeted Visa, PNC Financial Services Group Inc., Transamerica, New York Life Insurance Co. Synchrony Financial, and Trust Bank, and Twilio. As a financial organisation ourselves, we may end up as a potential target for foreign adversaries. Situated in a region that may experience geopolitical uncertainties in the near future (South China Sea), it would be our utmost priority to secure our assets for a potential cyber attack.

Threat 8: Man-in-the-middle attacks

If we scrutinise the techniques used for identity attacks in recent years, we would observe that more than 99% of identity attacks are password attacks, involving techniques such as breach replay, password spraying and phishing, that rely on predictable human behaviours such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.[7] However, these attacks often either have low success rates in the case of password spraying or, involve factors outside of our control in the case of phishing.



Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

More than 99% of identity attacks are password attacks

Breach replay

Password spray

Phishing

Rely on predictable human behaviors such as selecting easy-to-guess passwords, reusing them on multiple websites, and falling prey to phishing attacks.

<1% of attacks

Less than 1% combined

MFA attacks

SIM swapping

MFA fatigue

AitM

End-run MFA protection by intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve, and capturing first and second factor credentials using fake replicas of legitimate websites.

Post-authentication attacks

Token theft

Consent phishing

Infiltrate a user's account after they authenticate by stealing a legitimate token created on their device and moving it to a device under the attacker's control, by searching source code repositories for Open Authorization (OAuth) tokens and other non-human credentials, or by tricking the authenticated user into granting permissions to malicious apps.

Infrastructure compromise

Often silently executed by professional groups or nation-state-backed threat actors with sophisticated operations, making them very hard to detect. Threat actors may compromise an on-premises federation server and copy its private signing key to forge tokens, compromise a privileged cloud user and add new federation contracts, or compromise a non-human workload identity and create new credentials with elevated privileges.

Source: Microsoft Threat Intelligence

Microsoft (2024, p. 41)

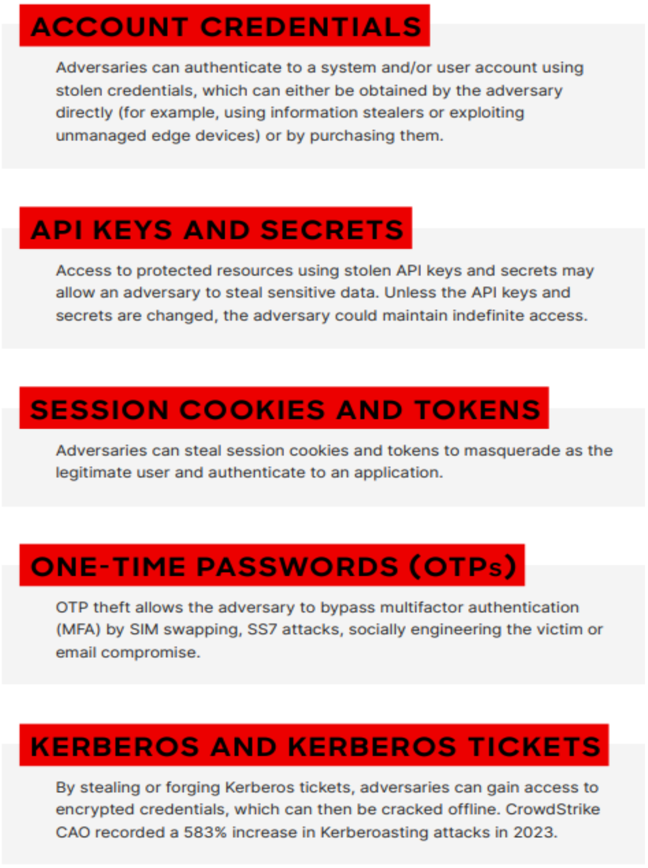
Although, for most of these attacks, adversaries would not be able to gain access to the accounts, unless they find a way to bypass Two-/Multi-Factor Authentication (2FA / MFA). Unfortunately, IBM X-Force responded to multiple cases involving email compromises that were able to circumvent MFA measures using adversary-in-the-middle (AitM) attacks. These attacks started with an initial phishing message that directed users to a reverse-proxy phishing page, which allowed attackers to relay traffic between the user and the legitimate site and thus collect user credentials, MFA input and session cookies.[5] If we, or any third-party supplier, were ever successfully threatened by an AitM attack, the adversary would be able to escalate their access using the techniques mentioned in privilege escalation and exercise other vulnerabilities, especially with identity attacks being so prevalent, causing non-insignificant damage to our organisation’s operations and reputation.

Cloudstrike has also observed that adversaries who use Man-in-the-middle attacks (FANCY BEAR; Russian cyber espionage group) have evolved and developed a custom toolkit to capture credentials from Yahoo! Mail and ukr.net webmail users. FANCY BEAR later expanded this toolkit to use the Browser-in-the-Browser technique in April 2023 and added MFA interception capabilities to its toolkit to collect OTPs sent to the MFA contact (e.g., a phone number) linked to the targeted account.[6]

However, most attacks bypass MFA protection by either intercepting security codes using stolen phone numbers, barraging users with MFA notifications until they approve or capturing first and second factor credentials using fake replicas of legitimate websites, and using the compromised credentials to gain access.

Threat 9: Social engineering

We continue to see identity-based attacks take center stage, as adversaries focus on social engineering attacks that bypass multi factor authentication. The use of legitimate tools to execute an attack, an increasingly prevalent technique, impedes the ability to differentiate between normal activity and a breach. To do this, they have continued to move beyond malware to faster, more effective means such as identity attacks (phishing, social engineering and access brokers) and the exploitation of vulnerabilities and trusted relationships.



ACCOUNT CREDENTIALS

Adversaries can authenticate to a system and/or user account using stolen credentials, which can either be obtained by the adversary directly (for example, using information stealers or exploiting unmanaged edge devices) or by purchasing them.

API KEYS AND SECRETS

Access to protected resources using stolen API keys and secrets may allow an adversary to steal sensitive data. Unless the API keys and secrets are changed, the adversary could maintain indefinite access.

SESSION COOKIES AND TOKENS

Adversaries can steal session cookies and tokens to masquerade as the legitimate user and authenticate to an application.

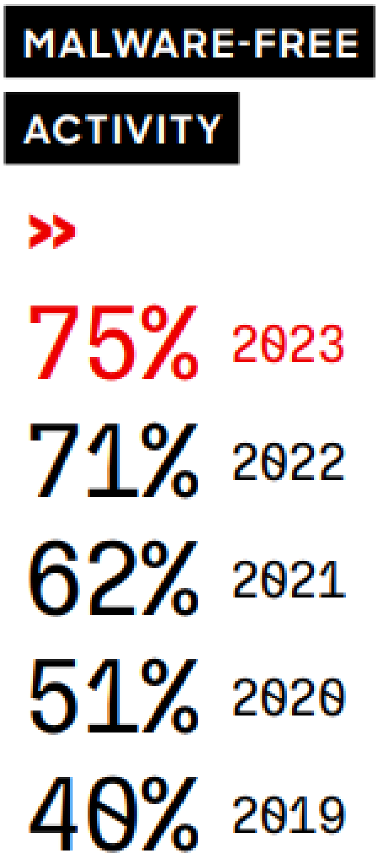
ONE-TIME PASSWORDS (OTPs)

OTP theft allows the adversary to bypass multifactor authentication (MFA) by SIM swapping, SS7 attacks, socially engineering the victim or email compromise.

KERBEROS AND KERBEROS TICKETS

By stealing or forging Kerberos tickets, adversaries can gain access to encrypted credentials, which can then be cracked offline. CrowdStrike CAO recorded a 583% increase in Kerberoasting attacks in 2023.

Figure 1. Identity-based attack vectors



This trend is apparent over the last five years, as malware-free activity represented 75% of detections in 2023 — up from 71% in 2022. This trend is partly related to the success of identity attacks, access brokers and the prolific abuse of valid credentials to facilitate access and persistence in victim environments. Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators.

These adversaries continued to profit from providing initial access to a variety of eCrime threat actors in 2023, with the number of accesses advertised increasing by almost 20% compared to 2022.[6]

Threat 10: Denial of Service attacks

Distributed denial of service (DDoS) attacks are commonplace in the current internet, where adversaries often abuse botnets to flood organisations with mostly garbage requests, have seen varying amounts of success, though usually affecting the smaller organisations much more. However, the goal of DDoS attacks are usually to either disrupt or disable a website or online service by overwhelming it with traffic from multiple sources. These attacks can cause significant losses for businesses such as downtime, lost revenue, damaged reputation, and increased costs.

Starting mid-March 2023, Microsoft reported an increase in network DDoS attacks, reaching approximately 4,500 attacks per day by June. A notable trend is the rise in application layer attacks targeting medium-sized applications, which are more sophisticated and stealthy than traditional network-level attacks. These attacks involve between 100,000 to 1 million packets-per-second, directly aimed at specific web applications, making them harder to detect and mitigate with standard volumetric DDoS protection methods.[7]

Potential Vulnerabilities

Using the weighted factor analysis worksheet, we have identified the top 10 assets in order from highest to lowest priority. Below is the table of vulnerabilities, its description and the type of assets it would affect.

ID	Vulnerability	Description	Type of asset affected
V1	Software not patched or updated	The software of the asset has not been patched or updated with the latest software, leaving us exposed to exploits that have already been patched	System Data
V2	Bad network segmentation	The poor network segmentation allows attackers to move laterally. Data can be easily accessed by attackers.	System
V3	Poor or lack of detection of target intrusion	Security systems do not detect when an attack occurs, allowing for a prolonged attack or further damage	System Data
V4	Inadequate protection against malware	The asset is not properly protected against malware. A simple malware attack could steal data or affect operations	System Data
V5	Weak or lack of access control	Inadequate access controls allow attackers and unauthorised employees to access system or data easily	System Data
V6	Inadequate mitigation strategies	Security measures that are insufficient, outdated, or improperly implemented. They cannot effectively reduce the impact of threats	System
V7	Poor incident response	Refers to delayed or inadequate actions, lack of clear communication, and failure to contain or mitigate	System Data

		the impact of an attack. This causes the attack to be unnecessarily more devastating	
V8	Inadequate monitoring of traffic	Without adequate monitoring of traffic, malicious activities will not be detected early.	System Data
V9	Inadequate firewall rules	Misconfigured or overly permissive firewall rules leaves the system or data more susceptible to attacks	System
V10	Weak endpoint security	Endpoints are targets for malware and ransomware. Weak security of them allow this attacks to occur easily and frequently	System Data
V11	Inadequate security measures from third-party partners	Attackers may exploit weak third party security measures	System Data
V12	Weak or lack of encryption	Data encryption ensures confidentiality. If it is weak or does not exist, data confidentiality is compromised.	System Data
V13	Lack of monitoring of employee activities	Without monitoring employee activities, we place ourselves at the risk of insider threats	System Data
V14	Lack of multi-factor authentication for VPN access	Attackers who compromise login credentials can easily gain unauthorized access to the VPN	System
V15	Phishing	Employees who fall for phishing scams may leak sensitive data or login credentials	System Data
V16	Poor education on social engineering tricks	Employees who are not well educated on phishing scams are likely to fall victim to them, compromising our security	System Data

	Lack of systems for handling traffic surges	Without proper systems for handling traffic surges, we are at risk of DoS and DDoS attacks	System
V17	Employees abusing access to VPN	Employees who abuse their access to the VPN essentially gain access to the whole network. They may be able to move laterally, increasing the risk of insider threat	System Data
V18	Failure to regularly back up data	Without regular backups, we risk losing important information in the event of a cyberattack or hardware failure.	Data

Based on the identified vulnerabilities, the previously identified threats could exploit the following vulnerabilities:

(Classified for TOP 10 asset previously identified)

- **Asset 1: Online Banking System Server**

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V6**: Lack of monitoring of employee activities **V7**: Poor incident response
Third-party vendor compromise [***T4***]	**V11**: Inadequate security measures from third-party partners
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V6**: Insufficient activity monitoring **V7**: Poor incident response **V12**: Weak or lack of encryption
Privilege escalation [***T6***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities
Cloud compromise [***T7***]	**V1**: Software not patched or updated **V2**: Bad network segmentation

	V5: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Weak endpoint security **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks
Denial of service attacks [***T10***]	**V6**: Inadequate mitigation strategies **V17**: Lack of systems for handling traffic surges

- **Asset 2: VPN Cloud**
    - **Note:** *This asset does **NOT** have a vulnerability for **SQL injection***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V6**: Lack of monitoring of employee activities **V7**: Poor incident response

Third-party vendor compromise [***T4***]	**V11**: Inadequate security measures from third-party partners
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V6**: Insufficient activity monitoring **V7**: Poor incident response **V12**: Weak or lack of encryption
Privilege escalation [***T6***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities
Cloud compromise [***T7***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Weak endpoint security **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks
Denial of service attacks [***T10***]	**V6**: Inadequate mitigation strategies **V17**: Lack of systems for handling traffic surges

- **Asset 3: Financial Transaction Data**
    - **Note:** *This asset does **NOT** have a vulnerability for **privilege escalation**, **SQL injection** and **denial of service attacks***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V19**: Failure to regularly back up data
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities **V18**: Employees abusing access to VPN
Third-party vendor compromise [***T4***]	**V2:** Bad network segmentation **V10:** Weak endpoint security **V11**: Inadequate security measures from third-party partners **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V7**: Poor incident response **V12**: Weak or lack of encryption
Cloud compromise [***T7***]	**V2**: Bad network segmentation **V5**: Weak or lack of access control **V10**: Weak endpoint security **V12**: Weak or lack of encryption

	V14: Lack of multi-factor authentication for VPN access
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks

- **Asset 4: Customer information**
    - **Note:** *This asset does **NOT** have a vulnerability for **privilege escalation**, **SQL injection** and **denial of service attacks***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V19**: Failure to regularly back up data
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities **V18**: Employees abusing access to VPN
Third-party vendor compromise [***T4***]	**V2:** Bad network segmentation **V10:** Weak endpoint security **V11**: Inadequate security measures from third-party partners **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V7**: Poor incident response **V12**: Weak or lack of encryption
Cloud compromise [***T7***]	**V2**: Bad network segmentation **V5**: Weak or lack of access control **V10**: Weak endpoint security **V12**: Weak or lack of encryption

	V14: Lack of multi-factor authentication for VPN access
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks

- **Asset 5: Customer Behavioural and Analytics Data**
    - **Note:** *This asset does **NOT** have a vulnerability for **privilege escalation**, **SQL injection** and **denial of service attacks***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V19**: Failure to regularly back up data
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities **V18**: Employees abusing access to VPN
Third-party vendor compromise [***T4***]	**V2:** Bad network segmentation **V10:** Weak endpoint security **V11**: Inadequate security measures from third-party partners **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V7**: Poor incident response **V12**: Weak or lack of encryption
Cloud compromise [***T7***]	**V2**: Bad network segmentation **V5**: Weak or lack of access control **V10**: Weak endpoint security **V12**: Weak or lack of encryption

	V14: Lack of multi-factor authentication for VPN access
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks

- **Asset 6: Firewalls (HQ and Branch firewalls)**
  - **Note:** *This asset does **NOT** have a vulnerability for **data breaches**, **SQL injection** and **man-in-the-middle attacks***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V10**: Weak endpoint security **V20**: Inadequate firewall rules
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities **V18**: Employees abusing access to VPN **V21**: Malicious or negligent employees altering firewall configurations
Third-party vendor compromise [***T4***]	**V2:** Bad network segmentation **V9:** Weak endpoint security **V11**: Inadequate security measures from third-party partners **V22**: Vendors misconfiguring or tampering with firewall

	settings
Privilege escalation [***T6***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities
Cloud compromise [***T7***]	**V2**: Bad network segmentation **V5**: Weak or lack of access control **V6**: Insufficient activity monitoring **V10**: Weak endpoint security
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks
Denial of service attacks [***T10***]	**V6**: Inadequate mitigation strategies **V17**: Lack of systems for handling traffic surges

- **Asset 7: CRM Server**

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V6**: Lack of monitoring of employee activities **V7**: Poor incident response
Third-party vendor compromise [***T4***]	**V11**: Third-party vendors with weak security measures
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V6**: Insufficient activity monitoring **V7**: Poor incident response **V12**: Weak or lack of encryption
Privilege escalation [***T6***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities
Cloud compromise [***T7***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Weak endpoint security

	V10: Weak endpoint security **V12**: Weak or lack of encryption
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks
Denial of service attacks [***T10***]	**V6**: Inadequate mitigation strategies **V17**: Lack of systems for handling traffic surges

- **Asset 8: Unreleased Financial Products or Services**
  - **Note:** *This asset does **NOT** have a vulnerability for **privilege escalation**, **SQL injection** and **denial of service attacks***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V19**: Failure to regularly back up data
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities **V18**: Employees abusing access to VPN
Third-party vendor compromise [***T4***]	**V2:** Bad network segmentation **V10:** Weak endpoint security **V11**: Inadequate security measures from third-party partners **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V7**: Poor incident response **V12**: Weak or lack of encryption
Cloud compromise [***T7***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V10**: Weak endpoint security

	V12: Weak or lack of encryption **V14**: Lack of multi-factor authentication for VPN access
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks

- **Asset 9: Intellectual Property and Trade Secrets**
  - **Note:** *This asset does **NOT** have a vulnerability for **privilege escalation**, **SQL injection** and **denial of service attacks***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V19**: Failure to regularly back up data
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities **V18**: Employees abusing access to VPN
Third-party vendor compromise [***T4***]	**V2:** Bad network segmentation **V10:** Weak endpoint security **V11**: Inadequate security measures from third-party partners **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V7**: Poor incident response **V12**: Weak or lack of encryption
Cloud compromise [***T7***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V10**: Weak endpoint security

	V12: Weak or lack of encryption **V14**: Lack of multi-factor authentication for VPN access
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks

- **Asset 10: Third-party and Vendor Information**
    - **Note**: *This asset does **NOT** have a vulnerability for **privilege escalation**, **SQL injection** and **denial of service attacks***

Threat	**Vulnerability**
Advanced Persistent Threats [***T1***]	**V1**: Software not patched or updated **V3**: Poor or lack of detection of target intrusion **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V6**: Inadequate mitigation strategies **V7**: Poor incident response **V8**: Inadequate monitoring of traffic **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Ransomware and malware [***T2***]	**V1**: Software not patched or updated **V4**: Inadequate protection against malware **V5**: Weak or lack of access control **V9**: Inadequate firewall rules **V10**: Weak endpoint security **V12**: Weak or lack of encryption **V19**: Failure to regularly back up data
Insider Threat [***T3***]	**V5**: Weak or lack of access control **V13**: Lack of monitoring of employee activities **V18**: Employees abusing access to VPN
Third-party vendor compromise [***T4***]	**V2:** Bad network segmentation **V10:** Weak endpoint security **V11**: Inadequate security measures from third-party partners **V12**: Weak or lack of encryption **V13**: Lack of monitoring of employee activities
Data breach [***T5***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V7**: Poor incident response **V12**: Weak or lack of encryption
Cloud compromise [***T7***]	**V1**: Software not patched or updated **V2**: Bad network segmentation **V5**: Weak or lack of access control **V10**: Weak endpoint security

	V12: Weak or lack of encryption **V14**: Lack of multi-factor authentication for VPN access
Man in the middle attack [***T8***]	**V8**: Inadequate monitoring of traffic **V10**: Weak endpoint security **V12**: Weak or lack of encryption
Social engineering [***T9***]	**V13**: Lack of monitoring of employee activities **V15**: Phishing **V16**: Poor education on social engineering tricks

Threats Vulnerabilities Assets (TVA) Worksheet

A Threat Vulnerability Asset (TVA) worksheet displays security vulnerabilities of our organization's systems, networks, or information assets in a table form. Conducting a TVA helps us prioritize assets based on its vulnerabilities present.

The x axis compromises of the top 10 most valuable assets identified in the weight factor analysis, and the y axis compromises of the top 10 threats identified in the potential threats section. For each asset and threat pair, a set of vulnerabilities is listed. If there are no vulnerabilities, a 'X' is placed instead.

	Online Banking Server	VPN Cloud	Financial Transaction Data	Customer information	CRM Server	Customer Behavioural and Analytics Data	Firewalls (HQ and Branch firewalls)	Unreleased Financial Products or Services	Intellectual Property and Trade Secrets	Third-party and Vendor Information
Advanced persistent threats (APT)	V1 V2 V3 V4 V5 V6 V7 V8 V9 V10	V1 V2 V3 V4 V5 V6 V7 V8 V9 V10 V13	V1 V3 V4 V5 V6 V7 V8 V9 V10 V12 V13	V1 V3 V4 V5 V6 V7 V8 V9 V10 V12 V13	V1 V2 V3 V4 V5 V6 V7 V8 V9 V10 V12 V13	V1 V3 V4 V5 V6 V7 V8 V9 V10 V12 V13	V1 V2 V3 V4 V5 V6 V7 V8 V9 V10 V13	V1 V3 V4 V5 V6 V7 V8 V9 V10 V12 V13	V1 V3 V4 V5 V6 V7 V8 V9 V10 V12 V13	V1 V3 V4 V5 V6 V7 V8 V9 V10 V12 V13
Ransomware and malware	V1 V4 V8 V9 V10	V1 V4 V8 V9 V10	V1 V4 V5 V9 V10 V12 V19	V1 V4 V5 V9 V10 V12 V19	V1 V4 V8 V9 V10	V1 V4 V5 V9 V10 V12 V19	V1 V4 V5 V10 V20	V1 V4 V5 V9 V10 V12 V19	V1 V4 V5 V9 V10 V12 V19	V1 V4 V5 V9 V10 V12 V19
Insider threat	V5 V6 V7	V5 V6 V7	V5 V13 V18	V5 V13 V18	V5 V6 V7	V5 V13 V18	V5 V13 V18 V21	V5 V13 V18	V5 V13 V18	V5 V13 V18
Third-party vendor compromise	V11	V11	V2 V10 V11 V12 V13	V2 V10 V11 V12 V13	V11	V2 V10 V11 V12 V13	V2 V9 V11 V22	V2 V10 V11 V12 V13	V2 V10 V11 V12 V13	V2 V10 V11 V12 V13
Data breach	V1 V2 V5 V6 V7 V12	V1 V2 V5 V6 V7 V12	V1 V2 V5 V7 V12	V1 V2 V5 V7 V12	V1 V2 V5 V6 V7 V12	V1 V2 V5 V7 V12	X	V1 V2 V5 V7 V12	V1 V2 V5 V7 V12	V1 V2 V5 V7 V12
Privilege escalation	V5 V13	V5 V13	X	X	V5 V13	X	V5 V13	X	X	X
Cloud compromise	V1 V2 V5 V6 V7 V8 V9 VI0 V12	V1 V2 V5 V6 V7 V8 V9 VI0 V12	V1 V2 V5 V10 V12 V14	V1 V2 V5 V10 V12 V14	V1 V2 V5 V6 V7 V8 V9 VI0 V12	V1 V2 V5 V10 V12 V14	V1 V2 V5 V6 V10	V1 V2 V5 V10 V12 V14	V1 V2 V5 V10 V12 V14	V1 V2 V5 V10 V12 V14
Man in the middle attacks	V8 V10 V12	V8 V10 V12	V8 V10 V12	V8 V10 V12	V8 V10 V12	V8 V10 V12	X	V8 V10 V12	V8 V10 V12	V8 V10 V12
Social engineering	V13 V15 V16	V13 V15 V16	V13 V15 V16	V13 V15 V16	V13 V15 V16	V13 V15 V16	V13 V15 V16	V13 V15 V16	V13 V15 V16	V13 V15 V16

Denial of Service attacks	V6 V17	V6 V17	X	X	V6 V17	X	V6 V17	X	X	X
Priority of controls	1	2	4	5	3	6	7	8	9	10

After visualising all the vulnerabilities, it is prioritised. While the priority mostly follows the order of importance in the weighted factor analysis worksheet, CRM server is prioritised over financial transaction data and customer information.

3rd highest priority CRM Server has potential vulnerabilities linked to all 10 threats identified, while 4th and 5th highest priority Financial Transaction Data and Customer Information respectively are not vulnerable to privilege escalation or denial of service attacks. Hence, while CRM server was deemed less valuable that the other 2, it has a greater attack surface and requires greater priority when implementing controls.

Risk Assessment

Risk assessment is a process that identifies and evaluates potential hazards and the risks associated with the highlighted assets. This is a crucial followup from the identification of risks, providing a more insightful look into the current controls in place and the inherent risks associated with the highlighted assets. The 5 assets deemed the most valuable are: Online Banking Server, VPN Cloud, Financial Transaction Data, Customer information, CRM Server. The assessment of risk is determined by analysing current controls, likelihood of execution and impact of successful execution.

Control Analysis

Control analysis refers to the review of the effectiveness of current existing controls in mitigating risks.

Online Banking Server

- Software not patched or updated: Risk under control = 0.6 (Moderate effectiveness due to automated patching)
- Lack of systems for handling traffic surges: Risk under control = 0.7 (Moderate due to only 2 routers being present to process traffic)

VPN Cloud

- Weak SSL/TLS configuration: Risk under control = 0.9 (Strong control due to enforced encryption)

Financial Transaction Data

- Poor detection of target intrusion: Risk under control = 0.9 (Strong monitoring systems in place)
- Weak or lack of encryption: Risk under control = 0.9 (Encryption policies mitigate most threats)

Customer Information

- Weak or lack of encryption: Risk under control = 0.8 (Moderate control via encryption enforcement)
- Lack of parameter queries: Risk under control = 0.7 (Moderate control but still susceptible to attacks)

CRM Server

- Lack of parameter queries: Risk under control = 0.8 (Moderate control but risk persists)

Likelihood Determination

Likelihood determination refers to the assessment of the probability of a vulnerability being exploited based on its exposure, historical trends, and security controls in place. Likelihoods are determined based on the value of the asset (how important it is to the attacker) and past year reports. This information may be referred to below.

Online Banking Server

- Software not patched or updated: Likelihood = 0.2 (Low probability due to existing update policies)
- Lack of systems for handling traffic surges: Likelihood = 0.6 (Higher probability, 2 servers in hq are used to handle traffic)

VPN Cloud

- Weak SSL/TLS configuration: Likelihood = 0.5 (Moderate probability, as weak encryption is commonly exploited)

Financial Transaction Data

- Poor detection of target intrusion: Likelihood = 0.3 (Low probability as monitoring is in place)
- Weak or lack of encryption: Likelihood = 0.5 (Moderate probability of interception)

Customer Information

- Weak or lack of encryption: Likelihood = 0.5 (Moderate probability due to potential vulnerabilities)
- Lack of parameter queries: Likelihood = 0.8 (High probability due to SQL injection risks)

CRM Server

- Lack of parameter queries: Likelihood = 0.5 (Moderate probability due to SQL injection attacks)

Impact Analysis

This section covers the extent of damage if a vulnerability is exploited. The higher the value, the larger the extent of damage. Similarly, these values are obtained from reports mentioned below.

Online Banking Server

- Asset Impact = 100 (Critical, as downtime affects all banking services)

VPN Cloud

- Asset Impact = 84.5 (High, as VPN ensures secure remote access)

Financial Transaction Data

- Asset Impact = 95.5 (High, as data breaches can cause financial fraud)

Customer Information

- Asset Impact = 93 (High, as data leaks harm customer trust and regulatory compliance)

CRM Server

- Asset Impact = 82.5 (Moderate to high, as CRM stores essential business data)

Ranked Vulnerability Risk Worksheet

The Ranked Vulnerability Risk Worksheet is crucial in identifying, assessing, and prioritising vulnerabilities in an organization's systems, networks, or applications. The table below neatly consolidates the information above and generates the inherent risk associated with each asset. This allows optimal allocation of resources and aids in the development of mitigation strategies to reduce risk.
The calculation for risk is:

(Likelihood of vulnerability occurrence x Value (Impact)) - Risk_under_control + Uncertainty

Asset	Asset impact	Vulnerability	Vulnerability likelihood	Risk under control	Uncertainty	Risk
Online Banking Server	100	Software not patched or updated Lack of systems for handling traffic surges	0.2 0.6	0.6 0.7	0.1 0.1	10 24
VPN Cloud	84.5	Weak SSL/TLS configuration	0.5	0.9	0.1	12.6
Financial Transaction Data	95.5	Poor detection of target intrusion Weak or lack of encryption	0.3 0.5	0.9 0.9	0.1 0.1	5.7 9.5
Customer information	93	Weak or lack of encryption Lack of parameter queries	0.5 0.8	0.8 0.7	0.2 0.1	18.6 29.7
CRM Server	82.5	Lack of parameter queries Software not patched or updated	0.5 0.2	0.8 0.9	0.1 0.3	12.3 6.6

The flow of the table is as follows: values on the far left refer to the assets, the headers asset impact, vulnerability and likelihood may be obtained from the above sections. These are crucial in determining the overall risk rating associated with each asset. However, we also need to calculate the posing risk by factoring in the current risk under control and uncertainty, these values may similarly be obtained above. Values are referenced from reports and statistics provided below.

Justification for uncertainty

Online Banking Server (Uncertainty: 0.1)

Online banking servers are typically well-monitored and maintained under strict compliance frameworks such as ISO 27001, NIST SP 800-53, and PCI DSS (for financial transactions).

VPN Cloud (Uncertainty: 0.1)

Robust industry standards such as VPN encryption protocols include TLS 1.3, OpenVPN, and IPSec and are integrated into systems across majority of organisations, hence the uncertainty level remains at 0.1

Financial Transaction Data (Uncertainty: 0.1)

Financial transaction data security is tightly regulated under compliance frameworks such as SWIFT CSP (Customer Security Programme) and PCI DSS.

Customer Information (Uncertainty: 0.2)

The uncertainty level is higher than other assets due to potential gaps in data governance, as customer data is stored across multiple systems as shown in the network diagram of DGT banks, leading to an increased risk of misconfigurations or accidental exposure.

CRM Server (Uncertainty: 0.1-0.3)

Most morden CRM servers have built in safeguards against parameter query related attacks such as SQL. Leading to a lower uncertainty level.

AS the CRM server is configured to be within HQ network, we may assume that an on-premise CRM software is used; hence the responsibility for patching, monitoring, and securing the database falls entirely on the organization. Delayed patching or outdated configurations introduce more uncertainty, leading to a higher uncertainty.

References

- Likelihood Values: These are derived based on industry knowledge of vulnerability exploitation and existing mitigations, mainly sources from OWASP Top Ten. For example, lack of encryption has a moderate likelihood (0.5) since attackers commonly exploit weakly encrypted data while unpatched software updates are less likely (0.2) due to strict policies within banking organisations such as DGT.
- Control Effectiveness: Stronger controls like encryption and monitoring have values closer to 1 (e.g., 0.9 for VPN encryption).
- Impact Scores: High values for customer information and financial transaction data indicate severe consequences of breaches. This is determined by taking into account the legal and reputational damage to the organisation should it be compromised.

Control Analysis

- OWASP Top Ten | OWASP Foundation. (n.d.). https://owasp.org/www-project-top-ten/

Likelihood Determination:

- National Institute of Standards and Technology. (2012). Guide for conducting risk assessments. In NIST Special Publication 800-30 (p. 95 pages). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Impact Analysis

- Cost of a data breach 2024 | IBM. (n.d.). https://www.ibm.com/reports/data-breach

Justification for uncertainty

- NIST Special Publication 800-53 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
- Perimeter. (2024, July 8). Encryption Standards for Business VPNs: Everything you need to know. Perimeter 81. https://www.perimeter81.com/blog/network/encryption-standards-business-vpn
- Requirement 4 - Prevent compromise of credentials - SWIFT Customer Security Controls Framework (v2022) on AWS. (n.d.). https://docs.aws.amazon.com/whitepapers/latest/swift-customer-security-controls-framework-2021/prevent-compromise-of-credentials.html

Risk Control

Risk Control focuses on identifying and implementing measures to address the risks identified during the assessment phase. After obtaining each risk value above, we need to systematically address each vulnerability depending on their function and purpose within the organisation and the rate of occurrence. This step effectively ensures that the organization proactively manages its risks associated with its assets while maintaining a secure and resilient environment. The list of potential strategies are as follows:

- **Avoidance/Defend**
- **Transfer**
- **Mitigate**
- **Accept**
- **Terminate**

To determine the appropriate risk control strategy, the organisation must first analyze each identified risk in detail, evaluating both its likelihood and potential impact against the organization’s risk tolerance and business objectives. By identifying and categorising the organization's assets, we may consider the list of potential strategies available to manage risk.

Each strategy has a specific focus:

- **Avoidance/Defend:** Eliminate or entirely avoid the risk source. This might involve discontinuing an activity or adopting alternative methods that do not introduce the risk.
- Transfer: Shift the risk to a third party, such as through outsourcing or insurance. This strategy is appropriate when a risk can be effectively managed by a specialist vendor or insurer.
- **Mitigate:** Implement controls to reduce the likelihood or impact of the risk. Common mitigation measures include technical safeguards like firewalls, encryption, or enhanced access controls.
- **Accept:** Acknowledge that the risk is within the organization's tolerance level and decide not to take further action. This is viable when the cost of additional controls exceeds the potential loss.
- **Terminate:** Cease the risky activity entirely if the risk cannot be adequately managed through other means.

Quantitative Analysis

To determine the strategies being implemented, we need to leverage the use of the CBA (Cost Benefit Analysis) worksheet. CBA is a form of a quantitative analysis assessment that helps to determine the feasibility and economic consequences of the highlighted vulnerability, allowing the organisation to take well-informed steps. The formula for calculation of the CBA is as follows:

SLE (Single Loss Expectancy) = **AF** (Asset Value) x **EF** (Exposure Factor)

ALE (Annual Loss Expectancy) = **SLE** x **ARO** (Annual Rate of Occurrence)

CBA = **ALE** (prior) - **ALE** (post) - **ACS** (Annual Cost of Safeguard)
(+positive indicate money saved)

Asset	**Risk**	**Asset Value**	**Exposure Factor**	**SLE**	**ARO**	**ALE**
Online Banking Server	Insecure configurations	$500,000	0.6	$300,000	0.5	$150,000
VPN Cloud	Insecure configurations	$200,000	0.5	$100,000	1	$100,000
Financial Transaction Data	Security Breach	$2,000,000	0.8	$1,600,000	0.2	$320,000
Customer information	Security Breach	$2,000,000	0.7	$1,400,000	0.2	$280,000
CRM Server	Operational Failures	$300,000	0.4	$120,000	0.5	$60,000

Asset	ALE (prior)	ALE (post)	ACS (annual cost of safeguard)	CBA
Online Banking Server	$150,000	$40,000	$80,000	+$30,000
VPN Cloud	$100,000	$15,000	$10,000	+$75,000
Financial Transaction Data	$320,000	$100,000	$50,000	+$170,000
Customer information	$280,000	$20,000	$12,000	+$272,000
CRM Server	$60,000	$20,000	$30,000	+$10,000

Justification

- **Online Banking Server**
  - Cost of safeguard should include measures and controls to prevent security breaches as it is the driving force of the company. Additionally, control practices must be in place to prevent operational failures and minimize downtimes to reduce financial losses and reputational damage
  - The +$30,000 reduction in potential losses shows the effectiveness of the safeguards implemented
- **VPN Cloud**
  - The remote gateway for employees, vendors and partners should be properly configured to prevent security breaches or employee mishandling. Safeguards and measures in place should be consisting of MFA (multi factor authentication), logging and strengthening of current existing controls to prevent unauthorized access.
  - The reduction in potential losses prove that it provides substantial monetary gain while maintaining a secure working environment
- **Financial Transaction Data**
  - Financial transaction data is a prime asset that, if exposed or manipulated, can lead to liability issues, fraud, and reputational damage Hence proper encryption and access controls must be implemented so as to prevent security breaches. Database encryption and access controls should cost around $30,000 with monitoring systems and staff costing around $20,000. Ensuring that optimal security are in place.
- **Customer Information**
  - Customer data, consisting of personally identifiable information (PII), is highly sensitive and often targeted for identity theft or resale on the dark web. Failure to uphold or secure these may leave the organisation with severe reputable damage that may greatly affect revenue and partner association.
  - Data masking and secure storage protocols/measures costs around $12,000 annually, this helps protect customer privacy and ensures compliance with legal requirements.
- **CRM Server**
  - The CRM server is vital for maintaining customer relationships and storing communication history. Downtime or data loss can disrupt business operations and harm client trust.
  - Frequent backups, storage systems and secure encryption policies, measures and protocols should cost $30,000 annually so as to ensure that critical customer data can be restored and protected in the event of an attack or hardware failure.

Regulation Compliance

Qualitative Analysis

Qualitative analysis is an alternative method to assess risks via evaluation of likelihood through non-numerical data. This method provides a foundation for assessing the effectiveness of existing controls and associated service costs while ensuring adherence to standards of due care and diligence to avoid legal or liability issues. This section will cover reports and other data-driven practices that the company can implement to maintain a secure and resilient environment. links to reports or references should be referred to in the **Appendix**

Local Compliance

The **Monetary Authority of Singapore (MAS)** provides comprehensive guidelines and policies to ensure financial institutions operate securely and mitigate risk through guidance in technology risk governance, security practices, and resilience for financial institutions.

- **MAS-TRM guideline 6.1.2:**

  “The secure coding and source code review standards should cover areas such as secure programming practices, input validation, output encoding, access controls, authentication, cryptographic practices, and error and exception handling”

  ➢ **Compliance with the above guideline** creates a security conscious environment that enhances the security of all assets, including banking servers, financial data and banking information

- **MAS-TRM guideline 6.1.6:**

  “It is essential for the FI to establish a comprehensive strategy to perform application security validation and testing. The FI may use a mixture of static, dynamic and interactive application security testing methods (refer to Annex A on Application Security Testing) to validate the security of the software application. The software validation and testing rules should be reviewed periodically and kept current”

  ➢ Banks should frequently improve their ability to detect and prevent scams by considering a broader range of scenarios and/or constantly improving their current measures. This ensures that they are consistently adhering to best practices and maintaining the asset’s integrity and security.

The **Personal Data Protection Act (PDPA)** provides a baseline standard of protection for personal data in Singapore. It complements sector-specific legislative and regulatory frameworks such as the Banking Act and Insurance Act. This Act must be mandatory for the organisation to adhere strictly to to avoid legal and civil liability.

- **PDPA Part 6.25 (Retention of personal data)**

- ➢ An organisation must cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —

- ➢ (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

- ➢ (b) retention is no longer necessary for legal or business purposes.

This section is especially critical for preserving the integrity and security of client's information and **personal data (PII)**. This policy may be applied in Financial Transaction Data, Customer information and CRM server.

Alternatively, the organisation may choose to adopt the GovZTA standard of Best Practices.The **Government Zero Trust Architecture (GovZTA)** provides a framework for the Singapore Government to implement Zero Trust; an architecture that assumes no user, application or device is trusted. Thus, adopting a layered defense approach throughout the stages of a cyber kill chain.

Global Compliance

Similarly, several sections under the **General Data Protection Regulation (GDPR)** are especially relevant and may serve as effective foundations for benchmarking in safeguarding data associated with the listed assets.

- **GDPR Article/Section 32**:

  "Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor, shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

  the pseudonymisation and encryption of personal data;

  the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

  the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

  a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing."

  - ➢ Compliance with GDPR Article 32 provides the company with proper standards such as encryption, pseudonymisation, and access controls to ensure the confidentiality and integrity of banking transactions and user data.
  - ➢ The article also emphasises on the timely ability to restore availability and access to personal data, making incident response strategies critical and enforced. This is especially critical in CRM servers and Online Banking Servers as it is crucial

that their services run undisrupted so as to minimise reputational and revenue loss.

- **GDPR Article 25**:

  "The controller shall implement appropriate technical and organisational measures to ensure that, by default, only personal data necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons."

  - **Article 25** ensures that safeguards like encryption and secure authentication (e.g., MFA) are built into the VPN and CRM server; protecting client/user data and preventing unauthorised access.

Similarly to the local branch, the hong kong branch of the organisation must adhere to their governance standards and regulations. This may be derived from the **HKMA guidelines (Hong Kong Monetary Authority)**, This Guideline is issued under **section 16(10) of the Banking Ordinance (the Ordinance)** and will take into account whether to authorize the organization applying to conduct banking business in Hong Kong. Hence the organisation **must** adhere to the these guidelines:

- Like conventional banks, a digital bank applicant must understand the types of risk to which it is exposed and put in place appropriate systems to identify, measure, monitor and control these risks. It should be aware that certain types of risk such as liquidity, operational (including protection of customer data) and reputation risk may be accentuated in the case of digital banks because of their nature of operation.

- **At a minimum**, the applicant must go through the eight basic types of risk identified in the risk-based supervisory framework of the MA (i.e. credit, interest rate, market, liquidity, operational, reputation, legal and strategic risk), analyse to what extent it will be subject to these risks as a digital bank and establish appropriate controls to manage these risks
  - The HKMA guidelines cover a strict set of measures to determine the security of the organisation through constant supervision. The organisation must follow the above listed steps such as "identify, measure, monitor and control" so as to run their branch in this region.

Enterprise Information Security Policy (EISP)

Executive Summary

At DGT, protecting the confidentiality, integrity, and availability of our customer and operational data is of utmost importance. This **Enterprise Information Security Policy (EISP)** establishes the foundation for safeguarding sensitive information, ensuring compliance with regulatory requirements, and fostering trust with our customers. DGT is committed to maintaining a robust security posture to protect against internal and external threats in the highly sensitive online banking sector.

If this is not prioritised, it could lead to the loss of customer trust and the reputation of DGT being tarnished.

Purpose

The purpose of this policy is to:

a. Define a comprehensive framework for managing and security DGT's information assets.
b. Assign clear responsibilities for maintaining and upholding information security.
c. Ensure compliance with relevant financial industry regulations, including:
    - **i. MAS TRM Guidelines**
    - **ii. General Data Protection Regulation (GDPR)**
    - **iii. Payment Card Industry Data Security Standard (PCI-DSS)**

d. Safeguard DGT's reputation and maintain customer trust by protecting sensitive data and ensuring secure operations.

Scope

This policy applies to:

a. People
- i. **All** employees of DGT, regardless of department or responsibility.
- ii. Contractors, consultants, and third-party vendors engaged with DGT.

b. Assets
- i. **All** information systems, networks, and data utilised in DGT's operations.
- ii. Customer information, regardless of format, such as paper-based or electronic.

c. Processes
- i. **All** activities and processes involved in managing DGT's operations, including online banking services and any supporting infrastructure.

Roles and Responsibilities

Executive Management

1. **Approve and Support the EISP**
    - Review and formally approve the EISP and any associated policies, ensuring that they align with organisational objectives and compliance requirements.
    - Allocate appropriate resources, such as budget, personnel and authorisation power to ensure the effective implementation of the EISP.

2. **Promote a culture of Security across the organisation**
    - Champion security initiatives to establish a top-down culture of accountability and awareness, regardless of department or responsibility.
        - Ensuring that everyone in the organisation is held responsible for security in their own domains, instilling a more nuclear management of security in the organisation.
    - Encourage transparent communication about cybersecurity risks, challenges, and achievements across all levels of the organisation. Ensuring clarity of the security posture of the organisation at all times, furthermore, keeping continuously aware of the security risks at hand.

Chief Information Security Officer (CISO)

1. **Oversee Implementation of the Security Program**
    - Develop, manage and continuously find flaws or areas of improvement to upgrade in the EISP in accordance with industry standards, regulations and organisational requirements.
    - Coordinate with other departments such as IT, HR and Legal etc., to integrate said developed security practices into all areas of the organisation. Furthermore, overseeing their proper and continuous implementation to achieve security.

2. **Regularly Review and Update Security Policies**
    - Conduct regular testing of all security-related policies to ensure that they are relevant, comprehensive and adaptable to emerging threats. This also prevents the current implemented policies from becoming obsolete and vulnerable to exploitation.
    - Incorporate feedback from audits, incident investigations, and regulatory updates into policy revision.
    - Ensure that the policies are communicated effectively across all stakeholders.

IT Security Team

1. **Monitor Threats, Apply Controls, and Manage Security Incidents**
    - Continuously monitor the organisation’s IT environment for potential threats and vulnerabilities using the security tools implemented and threat intelligence feeds such as SIEMs.
    - Implement, maintain, and update technical controls such as firewalls, intrusion detection systems, and endpoint protection. This ensures that these controls remain responsive to any form of threat and that they will operate as intended when need be.
    - Respond to and manage security incidents, including containment, eradication, and recovery efforts, while conducting proper documentation of the incident and performing proper reflection to ensure that the incident does not occur again.

2. **Conduct Regular Vulnerability Assessments and Penetration Testing**
    - Perform routine vulnerability scans to identify and remediate potential weaknesses in the organisation’s infrastructure, applications, and networks.
    - Engage in penetration testing to simulate real-world attacks, identify potential entry points and thereafter, validate the effectiveness of existing controls based on the findings.

Employees and Contractors

1. **Comply with Security Policies and Report Incidents Promptly**
    - Adhere to all security policies, standards, and procedures outlined in the EISP. Especially those related to data handling, access control and proper use of technology.
    - Promptly report any suspected or actual security incidents, such as phishing attempts, unauthorised access, or lost devices, to the IT security team. This allows for quick response to potential and active incidents, reducing the loss of company assets and time.

2. **Participate in Mandatory Security Awareness Training**
    - Complete all assigned security awareness training modules and refresher courses on time and properly.
    - Apply the principles learned in training actively in daily activities, such as recognising phishing attempts and safeguarding sensitive information.

3. **Fostering a Security-Conscious Work Environment**
    - Lead by example by consistently following security protocols and encouraging and holding peers accountable to do the same.
    - Share knowledge and tips from training with colleagues to enhance the collective security awareness within the organisation.

Third-Party Vendors

1. **Adhere to DGT's Vendor Security Standards and Contractual Obligations**
    - Comply with all security requirements as specified in vendor contracts, including adherence to security standards, data protection measures and reporting obligations. This reinforces the accountability that third-vendors have for the security on their own part, which collectively increases security for both parties.
    - Participate in regular security assessments conducted by DGT, such as audits, penetration tests, and compliance checks. Furthermore, being compliant with DGT intervention without hindering or disrupting their work.

2. **Ensure Security in Outsourced Processes and Services**
    - Implement robust security practices for any process or services outsourced to them, ensuring they align with DGT's security requirements.
    - Notify DGT immediately of any security incidents that could impact the organisation's data or systems.

3. **Support Continuous Risk Management**
    - Regularly evaluate and address risks related to their operations, products, or services, ensuring any issues are resolved in line with contractual agreements.

Policy Directives

Access Control

Rules-Based Access Control (RBAC)

- Implement RBAC to enforce the **principle of least privilege**, ensuring that users are granted access only to the information and systems necessary for their roles.
- Regularly review user access rights to ensure appropriateness, particularly when roles or responsibilities change.
- Use segregation of duties to prevent unauthorised or conflicting actions, such as combining access to both system administration and sensitive data.

Multi Factor Authentication (MFA)

- Require MFA for accessing all critical systems, including internal administrative systems and customer-facing platforms, to add an additional layer of security.
- Regularly review and update MFA mechanisms to ensure their resilience against evolving threats.
- Extend MFA to include privileged accounts, remote access, and cloud-based services.

Data Classification and Handling

Classification

- Data should be classified into the following categories based on its sensitivity and business impact:
  - Public - Information that can be freely shared without risk.
  - Confidential - Internal-use-only data that requires protection from authorised access.
  - Highly Sensitive - Critical business or personal data whose unauthorised access could result in severe financial, legal or reputational harm.

Data Handling

- Encrypt all Confidential and Highly Sensitive data during storage and transit using industry-standard encryption algorithms, such as **AES256** or **TLS1.3**.
- Implement robust key management practices to ensure secure generation, storage and rotation of encryption keys.
- Restrict data transfer to approved channels and prohibit unauthorised copying or sharing of sensitive data.

Incident Management

Incident Response Plan

- Maintain a detailed and documented Incident Response Plan (IRP) that outlines roles, responsibilities, and procedures for handling security incidents.
- Ensure that the plan covers detection, containment, eradication, recovery, and post-incident analysis.

Incident Reporting

- Require all employees, contractors, and vendors to report security incidents immediately to the IT Security Team via established channels.
- Utilise a centralised system for tracking and managing incidents, ensuring proper escalation and resolution.

Post-Incident Reviews

- Conduct post-incident reviews to analyse root causes and find loopholes that have been abused in existing controls and recommend improvements.
- Document lessons learned and update policies, procedures, and training programs if needed.

Risk Management

Annual Risk Assessments

- Perform comprehensive risk assessments annually to identify vulnerabilities in systems, process, and third-party relationships.
- Use risk assessment results to create a prioritised action plan for mitigating identified risks.

Risk Prioritisation

- Evaluate risks based on their potential impact on operations, financials, reputation, and compliance.
- Address high-impact risks with the highest priority, ensuring timely remediation.

Continuous Monitoring

- Monitor the risk landscape continuously to detect emerging threats and adjust mitigation strategies accordingly.

Compliance

Regulatory Compliance

- Ensure alignment with key regulations and standards, including:
  - MAS TRM Guidelines for technology risk management.
  - PCI DSS for payment card security.
  - GDPR for data protection and privacy.
  - National and international laws relevant to DGT's operations.

Audits

- Conduct regular internal audits to assess the effectiveness of security controls and compliance with policies.
- Engage third-party auditors to perform external reviews, ensuring an unbiased evaluation of compliance and security posture.

Training and Awareness

Mandatory Security Training

- Provide all employees, contractors, and third-party vendors with annual security awareness training, focusing on core topics such as:
  - Recognising phishing and social engineering tactics.
  - Secure data handling and password management.
  - Reporting security incidents and vulnerabilities.

Simulations

- Conduct regular simulation to test and enhance employees' ability to recognise and respond to security incidents, such as Phishing.
- Use the results in the simulation to identify areas where additional training or awareness efforts are needed.

Role-Specific Training

- Offer specialised training for employees with specific security responsibilities, such as system administrators, developers, and incident responders.
- Provide guidance to managers and executives on integrating security consideration decision-making processes.

Ongoing Engagement

- Use newsletters, posters, and interactive workshops to reinforce security best practices and maintain a high level of awareness throughout the year.
- Furthermore, this can be bolstered with constant efforts to adhere to best security practices and leading by example in the workplace.

Governance and Compliance

DGT is dedicated to maintaining the highest standards of security and compliance by aligning with both national and international regulatory frameworks and industry standards. The organisation’s governance and compliance strategy ensures that security practices are robust, transparent, and continuously improved. The key components of this strategy are outlined below:

Regulatory Compliance

1. **Monetary Authority of Singapore (MAS) Technology Risk Management (TRM) Guidelines:**
    - DGT strictly follows the MAS TRM Guidelines to manage technology risks effectively, ensuring that all systems, processes, and controls meet regulatory expectations for confidentiality, integrity, and availability.
    - Conduct regular self-assessments to measure compliance with MAS TRM requirements, such as incident response planning, cybersecurity measures, and outsourcing risk management.

2. **Data Protection Laws:**
    - Adhere to the Personal Data Protection Act (PDPA) to safeguard the privacy of individuals’ personal data within Singapore. This includes implementing data collection, storage, and processing measures that minimise risks of unauthorised access or misuse.
    - Comply with the General Data Protection (GDPR) for the protection of personal data belonging to EU citizens. This involves maintaining a lawful basis for data processing, providing transparency to data subjects, and ensuring data portability and erasure rights.

3. **Payment Card Industry Data Security Standard (PCI DSS):**
    - Ensure secure processing, transmission, and storage of payment card data in accordance with PCI DSS requirements.
    - Implement stringent access controls, encryption, and network security measures to protect cardholder data.
    - Conduct regular vulnerability scans and submit to periodic compliance assessments to maintain PCI DSS certification.

Internal Audits & Assessments

1. **Regular Audits**
   - Conduct regular internal audits to assess the effectiveness of implemented security controls, identify gaps, and ensure adherence to policies and procedures.
   - Engage independent external auditors to perform unbiased reviews of DGT's security posture, validating compliance with regulatory and industry standards.

2. **Penetration Testing & Vulnerability Assessments**
   - Perform penetration testing and vulnerability assessments at least quartely to proactively identify and remediate weaknesses in systems, networks, and applications.
   - Prioritise critical vulnerabilities for immediate resolution and document all findings and corrective actions in a centralised tracking system.

Policy Review & Updates

1. **EISP Review Schedule**
   - The EISP will undergo formal reviews biannually to ensure alignment with emerging threats, regulatory updates, and organisational needs.
   - Trigger additional reviews and updates following significant events, such as a major security incident, regulatory changes, or organisational restructuring.

2. **Authorisation & Approval**
   - All updates to the EISP will be drafted and authorised by the **Chief Information Security Officer (CISO**), who ensures the changes reflect the latest security requirements and best practices.
   - Executive management must formally review and approve the updates before implementation to ensure alignment with strategic and business objectives.

3. **Communication of Updates**
   - Communicate policy updates to all employees, contractors, and third-party vendors through formal notifications, training sessions, and updated documentation.

Risk Management Framework

1. **Structured Risk Identification & Evaluation**
    - Utilise a structured approach, based on **ISO 31000** standards, to systematically identify, assess, and prioritise risks.
    - Assess risk across all domains, including IT systems, processes, third-party relationships, and physical security, considering factors such as likelihood and impact on business objectives.

2. **Risk Mitigation & Monitoring**
    - Develop and implement mitigation measures for identified risks, assigning clear responsibilities and timelines for action.
    - Continuously monitor risks to detect changes in threat levels or vulnerabilities, ensuring risk management practices remain adaptive and proactive.

3. **Risk Register Maintenance**
    - Maintain a comprehensive risk register to document identified risks, associated impacts, mitigation measures, and status updates.
    - Use the risk register as a living document, reviewed regularly by the CISO and executive management to track progress and address unresolved risks.

4. **Incident Risk Evaluation**
    - Include incident findings and lessons learned in risk evaluations, updating risk profiles and mitigation plans as necessary.

Policy Enforcement

To maintain a secure and compliant, DGT enforces this policy through continuous monitoring, clear consequences for non-compliance, and structured incident response protocols. Enforcement measures are designed to ensure adherence to security standards while fostering a culture of accountability and proactive risk management.

Monitoring & Logging

1. **Comprehensive Monitoring**
    - Implement centralised logging and monitoring systems to capture all access attempts to sensitive systems, applications and data repositories.
    - Track user activities, including login attempts, data transfers, configuration changes, administrative actions, to create an audit trail that is able to support forensic investigations if needed.

2. **Audit & Review**
    - Conduct regular audits of logs and monitoring reports to identify unauthorised access, policy violations, or anomalous behaviour.
    - Retain logs for a minimum of one year or as required by regulatory mandates, ensuring availability for audit, compliance of legal review.

3. **Anomaly Detection**
    - Deploy anomaly detections tools and techniques such as Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) solutions, to identify potential breaches in real-time.
    - Set automated alerts for suspicious actions, such as multiple failed login attempts, access from unusual geographic locations, or large data transfers.
    - Use machine learning and behaviour analytics to enhance detection capabilities, adapting to evolving threats and user behaviours.

4. **Access Reviews**
    - Perform periodic access reviews to ensure that user permissions remain aligned with their current roles and responsibilities and configure access when needed.

Penalties for Non-Compliance

1. **Disciplinary Actions**
    - Violations of this policy by employees or third parties will be addressed through disciplinary actions which may include:
        - Verbal or written warnings.
        - Mandatory retraining or additional security awareness education.
        - Suspension or restriction of access to sensitive systems and data.
        - Termination of employment or contractual agreements in cases of severe or repeated violations.

2. **Legal Consequences**
    - Pursue legal action in instances of willful misconduct, negligence, or criminal activities, such as data theft, unauthorised access, or intentional damage to information systems.
    - Report incidents to relevant authorities and regulatory bodies as required by law, including data breaches that impact customer information or financial data.

3. **Third-Party Accountability**
    - Hold third-party vendors and contractors accountable for compliance with DGT's security policies and contractual objectives.
    - Terminate contracts with third-parties that do not uphold these principles or pose a continued security risk.

4. **Documentation of Violations**
    - Maintain a detailed record of all non-compliance incidents, including nature of the violation, disciplinary actions taken, and remediation measures implemented.
    - Use violation records for internal assessments and to inform policy updates or training enhancements.

Incident Response

1. **Documented Incident Response Plan (IRP)**
   - Handle all security incidents in accordance with DGT's documented IRP, which outlines the stages of incident management, including identification, containment, eradication, recovery, and post-incident analysis.
   - Assign roles and responsibilities within the IRP to ensure clear ownership and accountability during incident response activities.

2. **Immediate Reporting Requirements**
   - Mandate that employees, contractors, and third-party vendors report security incidents immediately to the IT Security Team via established communication channels.
   - Provide guidance on reporting different types of incidents, including data breaches, malware infections, insider threats, and physical security breaches.

3. **Response Procedures**
   - Initiate rapid containment measures to limit the impact of incidents, such as isolating affected systems, disabling compromised accounts, or blocking malicious network traffic.
   - Conduct thorough investigations to determine the root cause, extent of impact, and potential data exposure resulting from the incident.

4. **Communication & Escalation**
   - Establish clear communication protocols for informing relevant stakeholders, including executive management, legal counsel, and external parties, such as customers or regulators.
   - Escalate incidents based on severity, ensuring critical incidents receive ample attention and resources.

5. **Post-Incident Review & Improvement**
   - Conduct post-incident reviews to evaluate the effectiveness of the response, identify gaps in current procedures, and implement necessary improvements.
   - Update the IRP regularly based on lessons learned, emerging threats, and feedback from stakeholders.

Policy Maintenance

DGT's **Enterprise Information Security Policy (EISP)** will be continuously updated to address evolving threats, technologies, and regulatory requirements.

Review and Update Cycle

- Biannual reviews by the CISO and IT Security Team to ensure relevance and effectiveness.
- Immediate updates triggered by regulatory changes, security incidents, audits, or technology shifts.
- All changes will be documented, approved by executive management, and version-controlled.

Stakeholder Involvement

- Input from IT, Legal, HR, Risk Management, and Business Units to ensure comprehensive coverage.
- Employees can provide feedback through reporting channels, to ensure that all holes are plugged.

Change Management Process

- Formal approval process before policy changes take effect.
- Organisation-wide communication via email communications or intranet.
- Mandatory training sessions to ensure awareness and compliance.

Related Documents

The EISP is supported by the following policies and documents:

- **Acceptable Use Policy (AUP)**: Defines the acceptable use of DGT's IT resources.
- **Data Protection Policy**: Outlines guidelines for handling and storing customer and organizational data.
- **Incident Response Plan (IRP)**: Describes procedures for responding to security breaches or incidents.
- **Business Continuity Plan (BCP)**: Details actions to ensure service continuity in the event of a disaster or major incident.
- **Vendor Security Guidelines**: Specifies security requirements for third-party vendors and contractors.

Issue Specific Security Policy (ISSP)

Executive Summary

DGT bank recognizes and is aware of the growing threat landscape and is hence aware of the security of sensitive data regarding concerns of **unauthorised access**. This Issue Specific Security Policy (ISSP) establishes comprehensive guidelines and strategies for the implementation of secure storage, retention and protection of customer and financial data so as to prevent **unauthorised users from accessing sensitive data**. This section will further build up on the handling of sensitive data highlighted under the EISP and define clear strategies to mitigate risks. DGT Bank aims to uphold the confidentiality, integrity, and availability (CIA) of its data assets, reinforcing trust among customers, stakeholders, and regulatory bodies.

Purpose

The purpose of this section is to highlight and establish strict guidelines for the secure storage, retention, and protection of sensitive data at DGT Bank. It builds upon the general security framework established in the Enterprise Information Security Policy (EISP) and aims to address the risks raised such as unauthorised access to sensitive data and data interception. The goal of this policy is to ensure compliance with regulatory requirements and prevent unauthorized access. By enforcing proper data storage practices highlighted in this ISSP, DGT Bank aims to uphold the confidentiality, integrity, and availability (CIA) of sensitive financial and customer information.

Scope

This policy applies to:

- All employees, third-party vendors, and stakeholders handling sensitive data
- All digital and physical storage mediums used to retain sensitive information, including databases, file servers, cloud storage, external hard drives and physical tape or document archives
- Sensitive data, including but not limited to customer financial records, personally identifiable information (PII), transaction details, and internal corporate documents

Classification

The handling of sensitive data varies according to the data classification level mentioned in the EISP. This ensures that proper budgeting, financial resources and security controls are allocated according to the sensitivity level of the data and the security measures are proportionate to the risk associated with different data types.

- **Public:** No security controls required

- **Sensitive:** Internal business documents requiring controlled access
- **Confidential:** Customer banking details and transaction logs
- **Restricted:** Highly sensitive data such as encryption keys and access credentials

Storage Controls

Storage controls consist of encryption protocols and security specifications for data at rest and in transit be it on-site or off-site. This protects sensitive data from concerns such as unauthorised access as mentioned in the EISP, ensuring security and legal compliance.

- **Encryption:** All sensitive data must be encrypted using AES-256 (at rest) and TLS 1.3 (in transit).
- **Access Controls:** Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA) are required according to NIST 800-207.
- **Storage Security:** Data must be stored in secured, access-controlled environments, including on-premise servers or cloud platforms meeting ISO 27001 standards.

Retention and Disposal Policies

This section covers the retention timelines for different types of data and secure disposal methods, ensuring that the risk of a data breach while maintaining compliance is at a minimum.

- **Retention Periods:** Data must be retained for the minimum period necessary for business and regulatory requirements (eg, customer transaction records: 7 years per MAS TRM).
- **Secure Disposal:** End-of-life data must be securely erased using DoD 5220.22-M standard or physically destroyed.

Access Control

To maintain the security of sensitive data, access rights must be properly defined among employees or third party stakeholders, ensuring integrity and accountability of data.

- **User Access Management:** Employees must be granted access strictly based on job roles.
- **Multi-Factor Authentication (MFA):** Required for all privileged accounts.
- **Privileged Access Monitoring:** Logging and audit trails must be maintained for all administrative actions

Compliance

To ensure compliance, DGT Bank adheres to the following regulations and standards:

- **MAS TRM Guidelines:** Mandates robust IT security and data governance.
- **General Data Protection Regulation (GDPR):** Ensures protection of personal data and mandates breach notification procedures.

- **PCI DSS (Payment Card Industry Data Security Standard):** Enforces security controls for financial transactions.

Exceptions

Exceptions to this policy may be granted under the following conditions:

- A formal request is submitted to the **Chief Information Security Officer (CISO)** detailing the business justification and risk assessment.
- Approval is obtained from the **Security Steering Committee** after evaluating potential risks and compliance considerations.
- Temporary storage of sensitive data for specific business operations must adhere to strict security controls and be deleted immediately after use.

Non-compliance

Failure to adhere to this policy may result in severe consequences, including:

- **Disciplinary action**, up to and including termination, for employees found violating the policy.
- **Legal and financial penalties**, including fines for non-compliance with regulatory frameworks (eg, GDPR fines for data mishandling).
- **Increased risk of data breaches**, leading to reputational damage, loss of customer trust, and potential regulatory sanctions.
- Third-party vendors failing to comply will face **contractual termination and possible legal action**.

Related Documents

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. https://doi.org/10.6028/nist.sp.800-207

Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-5-gdpr/

Department of Defense. (2016). DOD 5220.22-M. https://sgp.fas.org/library/nispom/nispom2006.pdf

System Specific Security Policy (SYSSP)

Executive Summary

This section outlines the implementation plan and procedure for DGT Bank's System Specific Security Policy (SySSP) concerning the storage, retention, and protection of sensitive data. The purpose is to ensure regulatory compliance, data integrity, and confidentiality while mitigating risks associated with unauthorized access and data breaches.

Purpose

The objective of this section is to establish a structured approach towards enforcing security measures for sensitive data stored within DGT Bank's network infrastructure. The policy ensures that sensitive customer and financial data remain protected while aligning with industry standards, regulatory requirements, and internal governance.

Scope

The SySSP applies to:

- All sensitive data stored in DGT Bank's databases, cloud storage, CRM servers, and file archives.
- Employees, contractors, and third-party vendors with access to sensitive data.
- All hardware and software systems or infrastructure utilized for data storage and retention.

Implementation

Data Classification Policy

This section will cover the labelling and categorisation of data based on its sensitivity and impact. Proper classification of data ensures appropriate controls and security measures are implemented, maintaining the CIA of sensitive information. The implementation steps are as follows:

1. Identify and label sensitive data within storage systems.
2. Apply encryption and access restrictions to confidential and restricted data.
3. Conduct periodic data audits to validate classification accuracy.

Access Control Policy

Access control refers to the implementation of role based access control (RBAC) and multi-factor authentication (MFA) for data access. By Restricting access to authorized personnel, this effectively minimizes insider threats and unauthorized data breaches.

Implementation Steps:

1. Establish Access Control Policies: Define policies that dictate who can access specific data and under what conditions.
2. Implement Role Based Access Control (RBAC): Assign access permissions based on user roles within the organization.
3. Enforce Multi-Factor Authentication (MFA): Require MFA for accessing sensitive systems and data.
4. Regular Access Reviews: Conduct periodic reviews of access permissions to ensure they remain appropriate.
5. Logging and Monitoring: Implement logging and monitoring to track access to sensitive data and detect unauthorized access attempts.

Storage Control

This section covers the infrastructure and measures used to securely store sensitive data. The implementation steps to further ensure sensitive data is stored securely and maintaining the CIA triad is as follows:

1. Data Encryption: Encrypt sensitive data using industry-standard encryption algorithms such as AES-256
2. Secure Storage Solutions: Utilize secure storage solutions that provide access controls and monitoring capabilities.
3. Backup Procedures: Implement regular backup procedures to prevent data loss.
4. Physical Security: Ensure physical security measures are in place to protect hardware storing sensitive data.

Retention and Disposal Policy

Retention is defined as how long data should be kept and the proper disposal of said data when no longer needed. To prevent access to confidential outdated data and adhere to legal and regulatory requirements, documents and sensitive information must be properly destroyed using proper retention and disposal practices. Implementation and strategies are as follows:

1. Define Retention Periods: Establish retention periods for different data types based on legal, regulatory, and business requirements.
2. Automate Retention Enforcement: Use automated tools to enforce retention policies and delete data that exceeds its retention period.
3. Secure Disposal Methods: Implement secure disposal methods (e.g., data wiping, degaussing, physical destruction) for data that is no longer needed.
4. Documentation: Maintain records of data disposal activities for auditing purposes.
5. Regular Audits: Conduct regular audits to ensure compliance with retention and disposal policies.

Compliance maintenance

Lastly, to ensure that all listed strategies are adhered to, maintenance of compliance should be strictly adhered to with clear established policies, standards and guidelines. This ensures that the organisation is aligned with evolving security standards and regulations.

Implementation steps:

1. Regular Training: Provide ongoing training to employees on security policies and procedures quarterly. Training may include phishing simulations and tabletop excercises, exposing employees to understand security procedures.
2. Policy Reviews: Regularly review and update security policies to reflect changes in regulations and business practices.
3. Compliance Audits: Conduct periodic audits to assess compliance with security policies and standards.

Conclusion

The implementation of the Policies mentioned at DGT Bank are crucial in establishing a structured approach to mitigating risks, enforcing compliance, and safeguarding essential banking assets, such as customer information, financial transaction data, and online banking infrastructure. By integrating these policies into its security strategy, We can expect to enhance data protection, regulatory adherence, and operational resilience against evolving cyber threats within DGT Bank.

The importance of these policies is further supported by previous cyber incidents in Singapore's financial sector, such as the former assistant vice president at OCBC Bank. Between November 2022 and July 2023, he accessed the personal information of 396 customers without authorization. Utilizing the bank's Silverlake Integrated Banking System, he retrieved sensitive data—including NRIC numbers, dates of birth, addresses, contact numbers, bank account balances, and employment histories—pertaining to local politicians, public figures, colleagues, friends, and family members[1]. If similar attacks were to occur within DGT Bank, the ISSP and SySSP would provide critical safeguards, such as multi-factor authentication (MFA), real-time fraud monitoring, and employee awareness training

This incident underscores the critical importance of implementing robust Issue-Specific Security Policies (ISSP) to prevent unauthorized access by internal personnel. Such policies should enforce strict access controls, continuous monitoring, and regular audits to detect and deter unauthorized activities within the organization..

In conclusion, the implementation of the policies at DGT Bank is a proactive step towards securing financial assets, ensuring regulatory compliance, and maintaining customer trust. By reinforcing its cybersecurity measures, the bank can mitigate the risks of financial fraud, data breaches, and operational disruptions. The lessons learned from real-world cyberattacks emphasize the necessity of a continuous, adaptive security strategy, ensuring that DGT Bank remains resilient in the face of emerging threats. As cyber risks continue to evolve, the integration of these security policies will serve as a foundation for sustained digital trust and operational excellence.

Appendix

Assignment Resources:

Assignment https://nplms.polite.edu.sg/content/enforced/556448-24S2-1_CGRC_013844/CGRC%202024/CGRC-Assignment.pdf?isCourseFile=true&ou=556448

Rubrics

https://nplms.polite.edu.sg/content/enforced/556448-24S2-1_CGRC_013844/CGRC%202024/CGRC_Assignment%20Criteria%20Rubric_report.pdf?isCourseFile=true&ou=556448

Sources:

Clifton, C. (2024, November 6). Why Data Privacy Training Matters in Financial Services. *CISIVE*. https://blog.cisive.com/data-privacy-training-in-financial-services

Empowering and securing banking and financial organizations. (2023, August 28). https://live.paloaltonetworks.com/t5/general-articles/empowering-and-securing-banking-and-financial-organizations/ta-p/545427

Gammon, R. (2025, January 28). *Explained: The REAL impacts of data breaches for businesses*. Magna5. https://www.magna5.com/explained-the-real-impacts-of-data-breaches-for-businesses/

Koch, J. (2024, August 9). Financial Transaction Security: Mastering the Art of Digital Protection. *DivergeIT*. https://www.divergeit.com/blog/financial-transaction-security

Morin, C. (2023, May 21). The importance of data security in the financial services industry: Safeguarding Sensitive information -. *Qohash*. https://qohash.com/the-importance-of-data-security-in-the-financial-services-industry-safeguarding-sensitive-information/

Rundle, J. (2025, January 27). MGM Agrees to Pay $45 Million to Settle Data-Breach Lawsuit. *WSJ*. https://www.wsj.com/articles/mgm-agrees-to-pay-45-million-to-settle-data-breach-lawsuit-e076c842

Stevenwoodson. (2024, February 13). *Why financial services must prioritize privacy in service providers*. Brand Networks. https://bn.co/blog-posts/why-financial-services-must-prioritize-privacy-in-service-providers/

Team, C. (n.d.). *Data breaches: threats and consequences*. https://www.cloudmask.com/blog/data-breaches-threats-and-consequences

What can happen to your financial institution when data is breached | SQN Banking Systems. (2017, November 29). SQN Banking Systems. https://sqnbankingsystems.com/blog/can-happen-financial-institution-data-breached/

Risk Assessment:

1. Asset classification framework references: https://warwick.ac.uk/services/idg/im-policy-framework/standards/imst01/?utm_source=chatgpt.com
2. OWASP Top Ten | OWASP Foundation. (n.d.). https://owasp.org/www-project-top-ten/
3. National Institute of Standards and Technology. (2012). Guide for conducting risk assessments. In NIST Special Publication 800-30 (p. 95 pages). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf
4. Cost of a data breach 2024 | IBM. (n.d.). https://www.ibm.com/reports/data-breach
5. NIST Special Publication 800-53 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
6. Perimeter. (2024, July 8). Encryption Standards for Business VPNs: Everything you need to know. Perimeter 81. https://www.perimeter81.com/blog/network/encryption-standards-business-vpn
7. Requirement 4 - Prevent compromise of credentials - SWIFT Customer Security Controls Framework (v2022) on AWS. (n.d.). https://docs.aws.amazon.com/whitepapers/latest/swift-customer-security-controls-framework-2021/prevent-compromise-of-credentials.html

Risk Control:

1. SienceDirect. (December 2023). Exposure factors: https://www.sciencedirect.com/science/article/pii/S2772662223001686
2. SentinelOne. (2024, April 23). Cybersecurity in banking | Why cyber attacks on financial institutions are on the rise. https://www.sentinelone.com/blog/a-cyberwar-on-financial-institutions-why-banks-are-caught-in-the-crosshairs/

Regulation Compliance:

1. Monetary Authority of Singapore. (2021). Technology Risk Management Guidelines. https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
2. Government Zero Trust Architecture. (16 May 2023): https://www.developer.tech.gov.sg/guidelines/standards-and-best-practices/government-zero-trust-architecture
3. Personal Data Protection Act 2012 - Singapore Statutes online. (2022, October 1). https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P16-#pr24-
4. Art. 32 GDPR – Security of processing - General Data Protection Regulation (GDPR). (2016, August 30). https://gdpr-info.eu/art-32-gdpr/

5. Art. 25 GDPR – Data protection by design and by default - General Data Protection Regulation (GDPR). (2018, March 28). https://gdpr-info.eu/art-25-gdpr/
6. Monetary Authority. (2021). BANKING ORDINANCE authorization of digital banks. https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/guideline/Guideline_on_Authorization_of_Digital_Banks_eng.pdf

Threat Intelligence:

1. Aorato Labs. (2014). Target attack, step by step. https://aroundcyber.wordpress.com/wp-content/uploads/2014/09/aorato-target-report.pdf

2. Deconstructing the 2014 sally beauty breach. (2015, May 7). https://krebsonsecurity.com/2015/05/deconstructing-the-2014-sally-beauty-breach/

3. 6sense. (n.d.). Microsoft Active Directory - Market share, Competitor insights in identity and access management. Retrieved January 18, 2025, from https://6sense.com/tech/identity-and-access-management/microsoft-active-directory-market-share

4. Secure active directory and disrupt attack paths. (n.d.). https://www.content.shi.com/cms-content/accelerator/media/pdfs/tenable/tenable-041123-tenable-ad-datasheet.pdf

5. IBM. (2024). X-Force Threat Intelligence Index 2024. Retrieved January 18, 2025, from https://www.ibm.com/downloads/documents/us-en/107a02e952c8fe80

6. Kurtz, G. & CrowdStrike. (2024). CROWDSTRIKE 2024 GLOBAL THREAT REPORT. Retrieved January 18, 2025, from https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

7. Microsoft. (2024). Microsoft Digital Defense Report 2024. Retrieved January 18, 2025, from https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

8. Elastic Security Labs. (2024). 2024 Elastic Global Threat Report. Retrieved January 18, 2025, from https://www.elastic.co/pdf/elastic-global-threat-report-2024
9. "Snowflake Hacker Still Active, Finding New Victims, Expert Says". *Bloomberg.com*. September 20, 2024. Retrieved January 15, 2025.

IBM X-Force Threat Intelligence 2024:

https://www.ibm.com/downloads/documents/us-en/107a02e952c8fe80

Elastic 2024 Global Threat Report:

https://www.elastic.co/pdf/elastic-global-threat-report-2024

Sophos 2024 Security Threat Report:

https://assets.sophos.com/X24WTUEQ/at/wwf5phjtj9bjvmpqqsbfxc/sophos-2024-threat-report.pdf

Microsoft Digital Defense Report 2024:

https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf

CROWDSTRIKE 2024 Global Threat Report:

https://go.crowdstrike.com/rs/281-OBQ-266/images/GlobalThreatReport2024.pdf

MITRE ATT&CK® adversary tactics and techniques knowledge base:

https://attack.mitre.org

EISP

1. Monetary Authority of Singapore. (2021, January 18). Guidelines on Risk Management - Technology Risk. https://www.mas.gov.sg/regulation/guidelines/technology-risk-management-guidelines
2. General Data Protection Regulation. (2018, May 25). Information on GDPR. https://gdpr-info.eu
3. Office of Information Technology, M. (2014, March 7). Enterprise information security policy. https://www.mass.gov/doc/is000-enterprise-information-security-policy/download
4. Team Asana. (2025, Feb 1). Risk Register Maintenance. https://asana.com/resources/risk-register

ISSP

1. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero trust architecture. https://doi.org/10.6028/nist.sp.800-207
2. Art. 5 GDPR – Principles relating to processing of personal data - General Data Protection Regulation (GDPR). (2021, October 22). General Data Protection Regulation (GDPR). https://gdpr-info.eu/art-5-gdpr/
3. Department of Defense. (2016). DOD 5220.22-M. https://sgp.fas.org/library/nispom/nispom2006.pdf

Syssp

1. Tamper-proof logs | Identification for Development. (n.d.). https://id4d.worldbank.org/guide/tamper-proof-logs

Conclusion

1. Tham, D. (2025, January 3). Ex-OCBC assistant vice president jailed for unauthorised access to data of almost 400 customers. CNA.

https://www.channelnewsasia.com/singapore/ex-ocbc-assistant-vice-president-jailed-unauthorised-access-data-almost-400-customers-4836126