Summative Assessment

By GTB984, DXD946, KNM986, DXV925

In this exercise we create several documents for a hypothetical enterprise named “Swift Publishing”: a small internet-based desktop publishing company that prints business cards and advertising material. This Includes:

1. Security Policy
2. Risk Treatment Plan
3. Residual Risk Statement

We are developing these based on the original risk assessment document created for our formative assignment. This document is not considered gospel however and ideas have changed and improved as we have learned more for the module. We have also been taught several new methods.

Again, as with the risk assessment, we have made several assumptions about this enterprise in order to assess the relevant threats:

- The enterprise hosts a relatively well-known proprietary web application using its own servers.
- The web application is connected to a back end that automates the printing process without need for human intervention.
- The enterprise owns its own printing equipment but contracts another company for maintenance.
- The enterprise employs its own small network administration team.
- The company makes a steady profit but does not have the funds for vast equipment overhauls, updating occurs only when necessary.
- The hierarchy of the business is consistent with the real-world.

Security Policy for Swift Publishing

1. Scope

- This policy is relevant to Members of Staff, Contractors, Suppliers and Customers. However, this policy only applies to Members of Staff (including On-Site Contractors).

2. Definitions

1. For the purposes of this document, and all associated documents, the following definitions apply:

- Company - Refers to Swift Publishing.
- Members of Staff, Employee – All Staff currently under the employ of the Company.
- Contractor – An organisation providing a service to the Company.
- On-Site Contractor – An individual from a Contractor who is on the premises of the Company.
- Employee – Staff who exist on work registers and are officially tied to the company.
- Leaving Employee – Employees with an end date for their contract that is within one month.
- Ex-Employee – Members of staff who stopped working with the company within the last twenty-four months.
- Customer – Any person or entity that purchases goods and/or services from this company.
- Supplier – Separate Businesses that provide goods and/or services to this company.
- Visitor – Any individual who is not a Member of Staff who is on the premises of the Company.

3. Key Principles and Objectives

1. Company physical assets will be secured when unattended.
    - Assets must be physically secured, marked, and/or remotely monitored.
    - The appropriate level and means of protection will be defined for all physical assets.

2. The Company website and customer support facilities will be available within advertised times, except in the instance of:
    - Planned outages submitted in accordance with defined procedure, or,
    - Unavoidable outages, as defined in the residual risk statement.

3. Company information technology will be secured via a user authentication system.
    - Users will only have access to system resources required for their role.
    - The authentication process will secure systems against unauthorised access.
    - Externally accessible customer accounts will be processed separately from Company sensitive data.

4. Visitors to Company premises must be authorised.
    - On-Site Contractors and other visitors must obtain prior permission to enter the premises
    - Background checks must be run or requested for expected visitors
    - Unannounced visitors must be accompanied by Company personnel

5. The Company will use a Trusted Cloud Provider to store and process sensitive data.
    - The Trusted Cloud Provider will be unable to read or meaningfully modify sensitive data.
    - The Company will use secure channels to access the trusted cloud provider database.

6. The Company will make regular backups of operational data to the Trusted Cloud Provider.

7. The Company will monitor the release of security patches for Company software.
    - A system will be in place to assess any complications involved in the patching process

- Software that can no longer be guaranteed to be secure must be reassessed and replaced if necessary. Users of the software must be consulted as part of this process.
- The Company will identify and prioritise any patches that address critical vulnerabilities

8. Members of Staff will be trained in the importance of security within the Company.
   - Training will include the motivation for security measures wherever possible.
   - An easily accessible point of contact for Members of Staff with security concerns or queries will be available.

9. Staff appraisals will include an opportunity for staff to express discontent with company policy.

10. Leaving Employees will participate in a Security Exit Meeting. This meeting involves:
    - An audit of Company Assets in the possession of the Leaving Employee
    - An audit of Company credentials known by the Leaving Employee
    - The creation of a plan to retrieve identified assets and revoke identified credentials

11. Proposed changes to any security controls defined by, or subordinate to, the Principles and Objectives defined by this document must be approved by the CEO prior to implementation.

Risk Treatment Plan

Control	Threat Level	Control Description and Implementation Approach
Misuse of (business) network connections (internal & external)	Medium/High	The network could be misused by both internal and external threat actors. Employees may misuse the network for their own gain. External actors may mount attacks upon the network. Mitigations: • *Use a firewall, automated load balancing, and IP banning.* • *Use extensive logging. Use alert mechanisms to ensure that potential attacks and misuse recorded in logs are noted by staff.* • *Use a cloud-based service; these services have significant resources to defend against attack.* • *Ensure web-facing database uses prepared statements, input sanitisation, and other appropriate security measures.* • *Use well-established and maintained proprietary software, or well-established libraries when writing bespoke software.* • *Redundant Servers off-site or on alternative platforms.* • *Special selection of ISP based on their resilience.*
Tampering with equipment (hardware reconfiguration or theft)	Low/Medium	On-Site Contractors could tamper with machines to install new hardware that may alter the system to perform unauthorised actions, e.g. send sensitive data to a remote host or receive instructions from an external threat actor. Equipment may be physically stolen. Sensitive information could be taken from the premises through the theft of hardware or the use of removable data storage (USB flash drives etc). Mitigations:

		• *Maintenance records maintained and cross-checked against equipment in regular audit.* • *Access control cards used throughout the site.* • *Unused ports covered or removed; Lock in cables used where possible.* • *Software security policy countermeasures to prevent unauthorised port use/changes.* • *Whitelist firewalls automatically block unauthorised inbound traffic.* • *User account system only permits appropriate individuals to access sensitive data.* • *Redundant and/or spare equipment stored in multiple locations.*
Power Outage/Failure	Medium	The cause of power outage may be external to the company and difficult to control; however, there will need to be systems in place that allow the company to continue to operate with minimal disruption or, in the case of prolonged power failures, to execute a controlled shutdown of sensitive equipment. Mitigations: • *Have a backup generator and/or UPS system with automatic switch over.* • *Strict backup schedules.* • *The use of a cloud provider will ensure that only minimal data is lost in a catastrophic power failure.*
Damage to potentially exposed information infrastructure	Low/Medium	Information infrastructure external to buildings ("Potentially Exposed Infrastructure") could be tampered with, maliciously or accidentally. Potentially Exposed Infrastructure includes Company connections to the ISP, site CCTV, car park card readers, and all interconnecting cabling and wireless devices involved. Because it is external to buildings, it is more vulnerable. Disruption to the company connection to the ISP could result in significant downtime. Potentially Exposed Infrastructure is a target for threat actors who may be able to use it to directly monitor or interact with our network or security systems. Construction work on or next to the premises could damage or destroy this infrastructure.

		Cabling and associated equipment can be valuable and could be stolen. Mitigations: • *Protective casing around cables to reduce potential for damage.* • *Potentially Exposed Infrastructure to be consistently included in audit.* • *Fibre-optic cables are resilient and harder to breach with a man-in-the-middle attack. They should be used instead of copper cables.* • *Records must be kept of all underground cables on the premises. These records must be consulted when construction work is planned.* • *Wireless infrastructure to be appropriately secured.* • *Traffic arriving over Potentially Exposed Infrastructure should be firewalled.*
Leaving Employees	Medium/High	The Company will ensure that when Employees are leaving the company a Security Exit Meeting is conducted. This ensures that the Leaving Employee does not have any access to any of the company resources, and that sensitive Company and client data is protected. Mitigations: • *Security exit meeting* • *Audit of company assets and company credentials* • *Plan to retrieve identified assets and revoke identified credentials* • *Employee will be removed from the user authentication system* • *Network credentials* • *Email credentials* • *Cloud provider credentials*

Residual Risk Statement

Risk Omitted	Reasoning for Omission
Exploitation of zero-day vulnerabilities in Company software or use of highly advanced or obscure attack strategies against the Company network or web platform.	The expense needed to keep the firewall system plus supplementary hardware and software on the bleeding edge would be too great in relation to the cost of a security breach. Hardware will be updated at a slower rate as soon as is economically viable. **Alternative options** • Contract a security firm to handle our network security. • Contract a penetration testing organisation to regularly test network security in conjunction with realistic analysis and evaluation of findings.
Employees sharing identification and authentication tools.	Policy states that Members of Staff should not share passwords. Shared passwords represent a significant security breach as an unauthorised user could have access to privileged systems. However, as a company we are unable to monitor if Members of Staff are sharing their passwords with others. We will be able to monitor when a user account is accessed but will not know if the individual using those credentials is entitled to them. We also recognise that, in extenuating circumstances, the controlled sharing of passwords may be the least insecure solution to difficult problems. The same principles apply to physical means of authentication such as key fobs and access cards. **Alternative options** • Biometric identification technology for staff workstations and doors. • Creation of a temporary access control transfer mechanism.
Misuse of web platform and file storage solution (cloud storage)	The Company uses a cloud storage solution to store sensitive information and to backup all data. There should be no issue if the cloud storage solution is compromised as all data will be encrypted. The cloud provider will have backup systems in place to ensure redundancy, but breaches that occur on the cloud storage system are out of the Company's control.

	We are forced to trust that the cloud company, in their best interest, will not maliciously use our data, and will ensure their systems are secure to protect their business and reputation. **Alternative options** • Use of CryptDB system to further increase the cryptographic security of our cloud stored database.
Bribery or blackmail of Employees	The information considered ‘sensitive’ by the Company is generally more easily obtained elsewhere and is not likely to be considered very valuable to a potential threat actor. The Company is currently a relatively small player in the market and is not associated with any large businesses. However, while the likelihood of our Employees being approached by a threat actor with bribes or threats of blackmail is low, it cannot be discounted entirely. We have policy in place that allows staff to express their discontent with Company policy and the workplace environment, including a whistleblower scheme and regular appraisals with wellbeing-focused aspects. This reduces the likelihood that our Employees will accept bribes, but we cannot guarantee that Employees will not become disgruntled. More detailed monitoring of Employee behaviour will be counterproductive as it demonstrates bad faith. **Alternative options** • Offer Employees a comprehensive welfare and mental health service with links to outside agencies. • Perform detailed background checks and psychological evaluations of current and prospective Employees. • Monitor Employee activity and behaviour with the Company CCTV system.
Phishing and ransomware emails	The Company regularly receives phishing email. While Employee training briefly addresses the subject, we cannot realistically expect all our Employees to be able to accurately identify phishing email. Furthermore, while our email system includes filters that detect and isolate phishing email, this technology is imperfect.

	Our regular backup scheme and cloud-based storage offer us significant protection against ransomware attacks. If we are subjected to such an attack, we can roll back our information infrastructure with minimal loss of data. **Alternative options** • Logically and physically isolate different parts of the Company network. • Purchase more sophisticated phishing filter and anti-malware software. • Introduce further, mandatory security training for our Employees.
The long-term effects of the climate change disaster	The climate crisis is a slowly evolving process and is difficult to account for. Changes in society and the economic landscape related to climate change may significantly affect the Company in the future, but it is difficult to put controls in place for these changes. **Alternative options** • Creation of a Company environmental policy establishing strong Company responsibilities in the area of climate change. • Actively support environmental initiatives. • Actively consider climate change mitigation as part of all Company policy. • Actively monitor the current state of affairs in climate change and make policy changes based on developments as they occur. • Reduce use of unsustainable resources and utilities (e.g. wood paper, industrial glue). • Invest in renewable business operations as part of the company portfolio.
Large scale infrastructure destruction (Severe natural disaster, war, terrorist attack, nuclear incident)	The Company cannot predict or protect itself against severe natural disasters or international conflict. Our infrastructure and premises, such as buildings, computers, and printers, could be severely damaged and cost a lot of money to repair. Some of these events are severe enough that, in the event of their occurrence, the immediate restoration of Company services would not be a priority. The likelihood of these events occurring is low, and the company would not be able to assume the cost of their mitigation.

	Alternative options • Extensive structural survey and building reinforcement process. • Alternative, non-local premises made available for emergency use. • Cloud service provider in separate country/continent.