Assignment Guidance and Front Sheet

This sheet is to be populated by the Module Tutor, checked by the Programme Team, and uploaded to Moodle for students to fill in their ID and submit with their assessment.

Student ID or IDs for group work	**U2136249**

Module Title & Code	WM244 - Information Security Management
Module Owner	Dr Olga Angelopoulou
Module Tutor	Elzbieta Titis
Module Marker	Elzbieta Titis
Assesment type	CW1: Report
Date Set	10.10.22
Submission Date (excluding extensions)	07.12.22
Marks return date (excluding extensions)	20 working days from the submission date
Weighting of mark	50%

Assessment Detail	**The CISO memo** **Please see attached.**
Additional details	Your memo should not exceed 1500 words and follow an appropriate business memo format. Your article should cover the following sections: 1. Opening statement/ Executive summary 2. Severity of identified issues 3. The role of the CISO and the Cyber Security Team Organisational Structure and responsibilities 4. Importance of Data Protection and UK-GDPR 5. Recommendations You are expected to use appropriate peer reviewed sources for developing your arguments.
Module learning outcomes (numbered)	1 - Adopt a responsible attitude to the social, ethical, legal and regulatory consequences that flow from professional engagement in security management. 2 - Evaluate the overall coherence of an organisation's management of cyber security, recommending remediation where needed.
Learning outcomes assessed in this assessment (numbered)	1,2
Marking guidelines	You will be marked based on the following criteria: *1. Overview of your role and the proposed cyber security team* *2. Critical discussion on UK-GDPR and Data Protection Act in the context of an HE institution* *3. Memo organisation and conclusions* *4. Presentation, design and references – style and sources*

	Please also refer to the University Marking Scale (attached below).
Submission guidance	You must use the Harvard referencing system as per the University regulations. All submissions should be made in PDF format via Tabula https://tabula.warwick.ac.uk.
Academic Guidance	This coursework aims to guide you how to write a memorandum that reflects your understanding on specific areas of information security management and follow main academic writing principles. You are encouraged to use graphics, figures, and tables to make your memo more engaging for the reader. Additional guidelines if necessary will also be provided in a class briefing session.
Resubmission details	The University policy is that students should be given the opportunity to remedy any failure at the earliest opportunity. What that “earliest opportunity” means in terms of timing and other arrangements is different depending on Programme (i.e. Undergraduate, Full Time Masters, Part Time Postgraduate, or Overseas). Students are advised to consult your Programme Team or intranet for clarity.
Late submission details	If work is submitted late, penalties will be applied at the rate of **5 marks per University working day** after the due date, up to a **maximum of 10 working days** late. After this period the mark for the work will be reduced to 0 (which is the maximum penalty). “Late” means **after the submission deadline time as well as the date** – work submitted after the given time even on the same day is counted as 1 day late.

University of Cytroy

Business Memo

To: Executive team at University of Cytroy
From: Chief Information Security Officer
Date: 10/11/2022
Subject: Evaluate Current Information Security Posture of the Institution

Executive Summary

As the new Chief Information Security Officer (CISO), I am writing to inform you about the developments and implementation of a new information security program that will make sure all procedures and policies are compliant with the UK-GDPR and Data Protection Acts, ensuring the protection of all communications, systems, and assets from both internal and external threats against the University of Cytroy.

Context

Universities have always been at risk of cybercrime. During the years of 2020/21, in light of the world pandemic, higher institutions had to adapt and immerse themselves even more online, and with this, substantial new risks and challenges emerged. Universities collect valuable information varying from personal identifiable information (PII) of student data to the development of world-leading research, making them prime targets for cyber-attacks, which is why 75% of data breaches in the higher education sector happen at universities alone (GOV.UK, 2022).

Most of these cyber threats (90%) are caused by targeting staff and students rather than the cyber security defence systems already in place; these are known as phishing attacks. Therefore, focusing on training and awareness is critical to reducing the likelihood of data breaches from happening. Awareness campaigns are essential and should combine online-based training with in-person simulations, involving everyone in the organisation, from management staff to students. The goal should be to create a culture shift within the institution (Expede Group, 2022).

Due to the severity of student PII data being breached, the government has implemented security guidelines such as cyber essentials and policies like UK-GDPR that higher education institutes must adhere to; negating these can negatively impact universities, including hefty fines and operational restrictions.

Organisational Structure of a Cyber Security Team

Historically, organisations relied on only a few professionals in the Information Technology (IT) department dedicated to the security of their infrastructure. The global information security survey shows how organisations have neglected the management aspect of security and have blindly implemented security solutions without delegation of responsibility (KPMG, 2002). At the same time, breaches in security are becoming more noticeable and significant for both the public and private sectors.

The armed forces and financial services sectors were the first to begin the mission to take on an executive-level focus on security. They started by introducing an IT executive dedicated entirely to security, known as the Chief Information Security Officer (CISO), which bears the total weight of an organisation's security posture. As a result, IT executives worldwide are beginning to recognise that security responsibilities must be addressed at the management level to implement security within their organisations successfully. According to a recent study, 62% of Fortune 500 companies now have a CISO (bitglass, 2019), proving the need for a specialised role to protect all physical and technological assets of organisations.

CISO Responsibilities

CISOs handle the protection of all physical and technical aspects of the organisations. The SANS institute divides these aspects into four key functions:

1. **Protect, Shield, Defend and Prevent**: Proactively ensures the protection of the organisation's policies and technologies to defend against adversaries preventing the occurrence of cybersecurity incidents inline with the organisation's risk tolerance.
2. **Monitor, Detect and Hunt**: Actively monitor ongoing operations and hunt for and detect cyber threats and report all instances of suspicious or unauthorised events .
3. **Respond, Recover, and Sustain:** Minimise the impact and ensure all assets of the organisation are rapidly deployed, returning to normal operations when a cybersecurity incident occurs.
4. **Govern, Manage, Comply, Educate and Manage Risk**: Provide oversight, management and performance measurement of all cyber security functions, including all external and internal compliance requirements in line with the organisation's risk tolerance.

University of Cytroy

Business Memo

Figure 1 shows the formation of a new organisational structure of a cyber security team. Along with each role function, each department will have its own specific duties, function and responsibilities that will ensure the physical and cyber protection of all assets for the university of Cytroy.

Function	Department	Subfunction	Activities	Information Security Policy
Protect, Shield, Defend, Prevent	Application Security	Configuration Management	Manage Configurations for software and applications	Configuration and Change Management
Monitor, Hunt, Detect	Security Operations Centre	Virus and Malicious code Management	Detect, analyze, and eliminate viruses and malicuious code	Protection of software applications
Respond, Recover, Sustain	Emergency Operations and Incident Respond Centre	Incident Management and Response	Detect, analyse, respond to, and recover from suspicious events and security incidents	Security Incident Response
Govern, Comply, Educate	Program Management Office	Information Security Plan	Develop, Implement and maintain an information security plan	Information Security Plan

Figure 1

Current Cyber Security Posture

As my first step into the job, I took the initiative to review the past year's internal information security audit to evaluate the current security posture of the University. After analysing the audit I categorised and outlined below the ten most severe issues ranking them from most to least critical concerning physical and technical shortfalls:

1. *Limited documentation on information security procedures*
2. *Limited effort to raise security awareness*
3. *No clear structure of responsibilities in an event of a cyberattack*
4. *Unlocked computer systems*
5. *Unattended and unsecured portable devices*
6. *Limited audit log policies*
7. *Weak password enforcement*
8. *Out of date and expired antivirus software on internal servers*
9. *Elevated privileges to computer systems of some members of staff*
10. *Unauthorised software installed on University owned systems.*

Importance of an Information Security Policy

Security threats evolve at a rapid pace, making compliance requirements more complex. Thus, organisations must design a comprehensive Information Security Policy to cover both challenges. Information systems underpin the University's activities and are critical to its teaching, research, and administrative functions. So, all members of the University must ensure the availability, integrity, confidentiality, and authenticity of the information they hold or access. Misappropriation of information can potentially cause reputational damage and disruption to the University's business and expose the organisation to legal sanctions (ICO, 2022).

Elements & Implementation of an Effective Information Security Policy

During the security audit analysis, I discovered that the institution lacked one or more of the nine essential elements that make an effective information Security Policy, shown in Figure 2 (Exabeam, n.d.)

Element Objective	Implementation
Purpose	The university needs to state the purpose of the policy, which may be to: • Create an overall approach towards information security, including; standards, security requirements and practices adopted by the institution • Detect and prevent breaches such as; misuse of networks, data, applications and computer systems • Maintain the reputation of the institution by upholding ethical and legal responsibilities applicable to governance. • Respect and protect student and staff data rights.
Audience	The university must define whom the information security policy applies to. E.g - which audiences are out of scope of the policy.
Information Security Objectives	The university needs to focus on three main objectives: • **Confidentiality**: only authorised individuals can access data and information assets • **Integrity**: Data should be intact, accurate and complete. **Availability**: Users must be able to access information / systems when needed.
Authority and Access Control Policy	The policy needs to outline the level of authority over data and IT systems for different roles across the institution. E.g - Senior manager Vs Junior Employee. Students and Staff should only be able to access the institution's networks and servers via security authentication, which can include; passwords, biometrics or ID cards. The university must monitor all systems and record all login attempts.

Element Objective	Implementation
Data Classification	The university should classify data into categories. E.g - “Top Secret”, “Secret”, “Confidential”, and “Public”. Allowing the protection of highly important data, and avoiding needless security measures for unimportant data.
Data Support and Operations	Data storage systems that contain sensitive data, such as PII data must be protected according to the institutional standards. Common standards require; encryption, firewalls, and anti-malware protection.
Security Awareness and Behaviour	The university should carry out training and awareness sessions to inform all students and personnel of the current security procedures and mechanisms implemented. Including Data and access protection measures.
Encryption Policy	Encryption is vital to keep information inaccessible from unauthorised parties. By having an encryption policy, it helps the institution define the devices and media that must be encrypted, and ensure that sensitive and proprietary data remains private.
Backup Policy	Backups are an integral component of the overall data protection and business continuity of any organisation. The institution must: • Define all information of the university that needs to be backed up. • Determine the frequency of backups. • Defines a storage location. • List all roles in charge of backup processes.

Figure 2

Raising Security Awareness

> 95% of cybersecurity issues can be traced to human error (World Economic Forum, 2022)

As the new CISO, I propose developing a new awareness campaign designed to improve cybersecurity knowledge across the institution, raising awareness of threats and educating users to avoid cyber-attacks. The idea is to create a ‘culture of security compliance’ rather than provide ‘training’.

The campaign must start with an initial training tailored to each department. For university staff, a fundamental understanding of GDPR compliance would be crucial; staff have access to PII of students, so ensuring it does not become public is vital. For students, examining issues such as phishing attacks and avoiding malware-attacks will be more important. Training can take a mixed approach of video content, written guides, game scenarios along with constant feedback, which has been proved to be more impactful than a single-media approach.

A critical aspect of the campaign is to test users with simulated phishing emails and scams. Simulated scenarios involve a ‘fake’; phishing email sent to users to determine whether or not they will be tricked into clicking malicious links. Combining this with measurable metrics will enable the institution to identify the staff and students who still require more training, Creating cost-effective training in the long term, targeted for individuals who need it the most and develop a solid ‘human firewall’ that will cut off the problem right at the source, enabling the prevention of cyber-attacks from evolving in the first place.

Need for Competent Incident Response Team

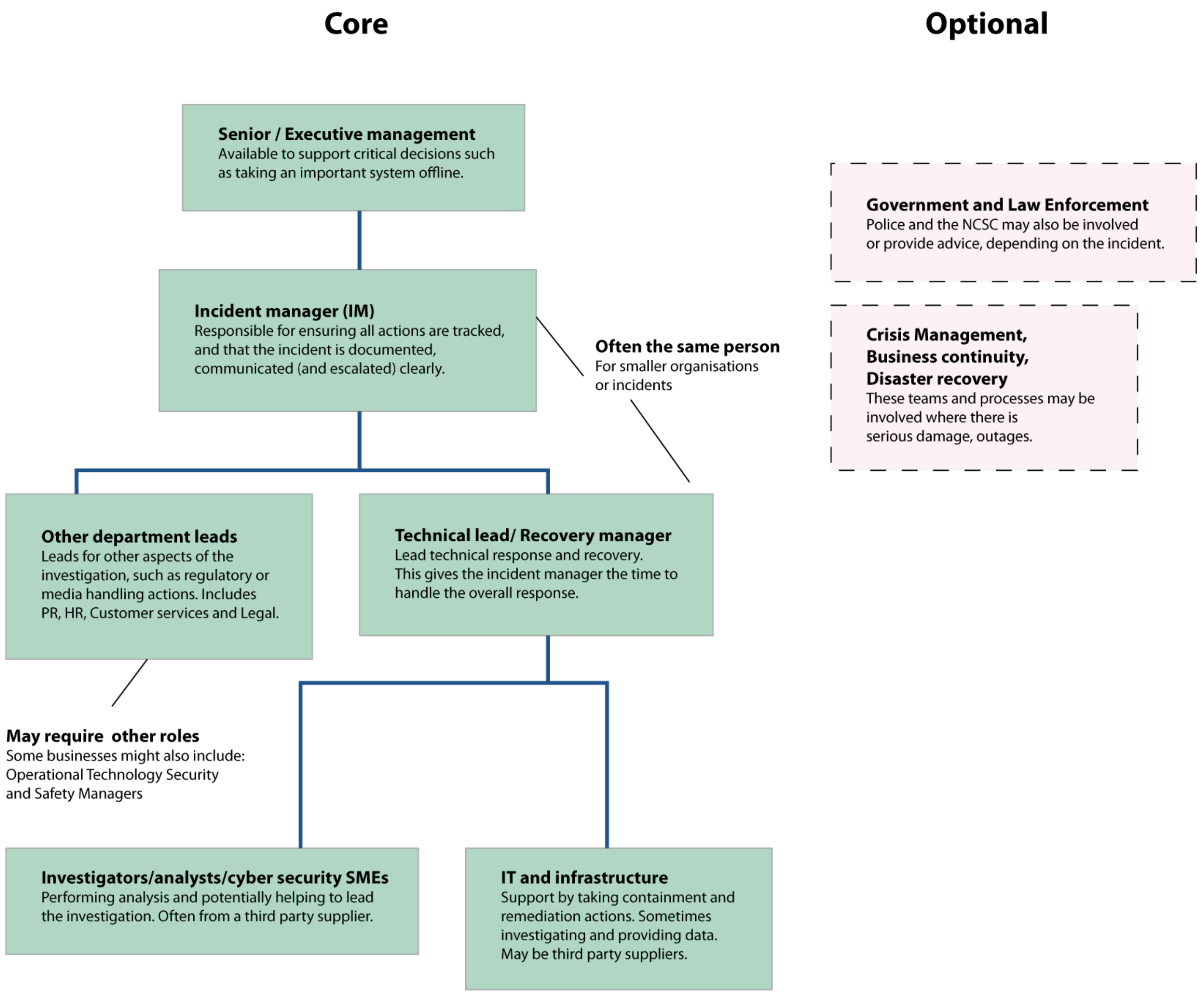
The aim of the Cytroy University must be to uphold an environment that ensures the confidentiality and integrity of student and staff data.

Although data breaches are inevitable, it is vital to have an effective cyber security incident response team (CISRT) on the premises, to keep information of the university intact. The team can be dedicated to something other than IR full-time. A more cost-effective approach is to have a 'virtual' CSIRT, pulled together when needed, from people who have other day jobs.

The CSIRT will require numerous roles to guarantee that incidents are managed and coordinated effectively. These fall under the headings (NCSC, 2019):

- *Government and law enforcement*
- *Executive Management*
- *Incident manager*
- *Recovery manager*
- *Disaster recovery & Crisis Management*
- *Investigators and Analysts*
- *IT and Infrastructure*
- *PR, HR and Customer Services.*

A detailed explanation is shown in figure 3:



Core

Optional

Senior / Executive management
Available to support critical decisions such as taking an important system offline.

Incident manager (IM)
Responsible for ensuring all actions are tracked, and that the incident is documented, communicated (and escalated) clearly.

Often the same person
For smaller organisations or incidents

Other department leads
Leads for other aspects of the investigation, such as regulatory or media handling actions. Includes PR, HR, Customer services and Legal.

Technical lead/ Recovery manager
Lead technical response and recovery. This gives the incident manager the time to handle the overall response.

May require other roles
Some businesses might also include: Operational Technology Security and Safety Managers

Investigators/analysts/cyber security SMEs
Performing analysis and potentially helping to lead the investigation. Often from a third party supplier.

IT and infrastructure
Support by taking containment and remediation actions. Sometimes investigating and providing data. May be third party suppliers.

Government and Law Enforcement
Police and the NCSC may also be involved or provide advice, depending on the incident.

Crisis Management, Business continuity, Disaster recovery
These teams and processes may be involved where there is serious damage, outages.

Figure 3

Protection of Hardware & Software Resources

My role as the CISO is to protect the institution's physical and technical aspects. For this reason, I propose a set of new standards that will help the university of Cytroy to ensure the compliance and security of all assets. Figure 4 shows what the University of Cytory must do to comply with GDPR and the data protection act.

Cyber Security Standard	Satandard Importance	How to meet Standard	Technical Requirements
Protection of Devices on every network	Well defined firewalls will prevent many attacks from occurring. They can also make scanning for suitable hackable targets much harder.	Monitor logs and document decisions made on inbound traffic.	• Protect hardware devices with a correctly configured firewall. • Change admin password and remote access. • Protect firewall admin interface with multi-factor authentication (MFA). • Keep firewall firmware up to date.
Accounts should only have the access they require	Successful cyber attacks target accounts with the highest privileges. By limiting the number of access points on the network of global admin accounts, the institution can prevent and limit successful attacks.	There must be a user account creation, approval and removal process.	Only certain authorised people can have an account that allows them to access, alter, disclose or delete held PII data.

Anti-Malware implementation on all devices across every network	Up-to-Date anti-malware and anti-virus software minimises the risk of a cyber attack	Administrate processes for risk-assessment, authorisation and documentation for any access to potentially malicious websites.	Make sure anti-malware: • Is set to scan files when downloaded or opened. • Scans websites when accessed • Prevent access to malicious web pages
Protection of accounts to sensitive or operational data	Sensitive and operational data if compromised, would have a serious impact on the overall security of the institution	Institution should implement and require multi-factor authentication (MFA) as well as strong password policies across the whole organisation	Multi-factor authentication should include: • Password with at least 8 characters made up with special letters / symbols: • Biometric authentication • Managed device by the institution • Authentication token via physical device or digitally by a trusted application
Devices must be patched with latest security updates	Attackers attempts to exploit vulnerabilities on outdated software, so making sure every system receives the latest security patches is crucial	Subscribing to services rather than buying allows the organisation to manage devices more easily, this is known as Software as a Service (SaaS)	Complete manual updates to hardware and software, within 14 days of security updates realise, prioritising patches where the vulnerability is: • Described as high risk • Has a Common Vulnerability Scoring System (CVSSv3) score of 7 or above.

Figure 4

Summary

In short, with the rise in security awareness, public and private corporations have turned to the CISO to solve their security issues. CISOs are high-level executives with the technical expertise necessary to implement security solutions and business knowledge to ensure that key decisions are aligned with the organisational mission. The CISO is necessary for effectively implementing security for any business.

The University of Cytroy must focus on creating a 'cultural of security compliance' across the institution to ensure compliance with the GDPR and Data Protection acts to avoid heavy fines and restrictions along with the protection of world-leading research and the PII of students and staff.

References

bitglass, 2019. Analysis of Cyber Security in the fortune 500 companies.
Exabeam, n.d. The 12 Elements of an Information Security Policy [WWW Document]. Exabeam. URL https://www.exabeam.com/explainers/information-security/the-12-elements-of-an-information-security-policy/ (accessed 12.2.22).

Expede Group, 2022. The Benefits of Cyber Security Awareness Training Within Universities [WWW Document]. URL https://edition.pagesuite-professional.co.uk/html5/reader/production/default.aspx?pubname=&edid=10ade5e1-f994-4092-9f34-b56d3552a72a (accessed 12.3.22).

GOV.UK, 2022. Educational institutions findings annex - Cyber Security Breaches Survey 2022 [WWW Document]. GOV.UK. URL https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/educational-institutions-findings-annex-cyber-security-breaches-survey-2022 (accessed 11.22.22).

ICO, 2022. Guide to the General Data Protection Regulation (GDPR) [WWW Document]. URL https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/ (accessed 12.6.22).

KPMG, 2002. Global Information Security Survey 2002 - Computer Business Review Africa [WWW Document]. URL http://www.cbr.co.za/article.aspx?pklarticleid=1743 (accessed 11.30.22).

NCSC, 2019. Build: A cyber security incident response team (CSIRT) [WWW Document]. URL https://www.ncsc.gov.uk/collection/incident-management/creating-incident-response-team (accessed 12.4.22).

World Economic Forum, 2022. The Global Risks Report 2022.