COMP1608: Information Security Management System

Trevor Kiggundu: 001001720
December 2020

A report submitted in fulfilment of the requirements for the module, Managing IT Security and Risk, Computing and Information Systems Department, University of Greenwich.

Table of Contents

1 Executive Summary and Business Unit Operations

The organization that is being proposed for study is a university library system. For the sake of the assignment, the university will be referred to as 'The Pluto University'. The business unit chosen to be specifically defined is the IT and technical support helpdesk within the library, as this specific university separates the roles of the library and IT staff respectively. The library aims to provide a suitable and interactive environment for learning, as both the traditional and technological aspects of learning evolve. The library and IT team also provide some of the most up to date facilities for the university students, staff and alumni to use. To keep in line with current times and to make the scenario somewhat realistic; the library also offers online/remote support for those that are unable to seek help in person during difficult times.

Defining stakeholders in an organization is important, as it allows for the relevant participants in a system to be identified; their input is also important as they provide feedback and help the project managers understand "project constraints and risks" (Schoenhard, 2019). The roles of the personnel vary from position to position, but all of the staff have a certain duty to the profession that they must uphold. There are senior members of staff that are essentially the heads of departments; they handle back end interactions and employ junior members that handle the more 'face to face' interactions. Described below are some of the customer service roles and responsibilities that all IT staff must be able to complete once called upon:

- Offer technical and user support for any queries brought along by the customers.
- Possess the relevant technical knowledge to help diagnose any hardware or software issues encountered by customers.
- Troubleshooting any unsolved queries that customers may have.
- Ensure that all customers are using the facilities, equipment and resources available to them appropriately and respectfully.
- Handle student records and sensitive information such as ID numbers, dates of birth, usernames and passwords, potential disabilities etc.

2 Key Assets

2.1 Scope

The scope of the ISMS is the management and protection of the commercial/ personal information that belongs to the students, staff and to all internal stakeholders directly involved with the Pluto University library and IT service system.

2.2 Policy

The purpose of the ISMS is to ensure that the information assets that are housed by the IT/Library system remain safe and useful. The system must also make sure to comply with consumer and corporate standards for data protection, as every stakeholder in the system has potentially sensitive information that could be subject to a potential security breach. Any compromise to a similar system is likely to cause an array of legal, ethical, professional and social issues. Serious breaches can also affect the systems entire ability to function; impacting the key assets of the specific system defeating the main purpose of the system, which is to safeguard those assets. In the event that any of these breaches unfortunately occur, the system must be able to respond to the threat in a timely manner to avoid further damage; no system is invulnerable to attacks. The system must make sure to treat internal threats as seriously as external ones, as they can potentially be as serious if overlooked. Finally, the ISMS must conform to standards agreed upon by all of the stakeholders involved, as well as be user-friendly enough for even the least technology friendly individuals to be able to use effectively. Discussed below are some of the key assets and other objectives for the Pluto University system.

2.2.1 Goals and Objectives:

- Prevent unauthorised access to computer material from external attackers and internal users.
- Prevent unauthorised access to personal information from external attackers and internal users.
- Proactively scan and monitor systems to avoid any internal/external threats from accessing the system.
- Respond effectively to the eventual inherent threats that will affect the system.

2.2.2 Key Assets

Key Asset	**Valuation**
Employee Personal Information	High: This information is inherent to a single individual and can put them at risk if revealed irresponsibly.
Student Personal Information	High: This information is inherent to a single individual and can put them at risk if revealed irresponsibly.
Company Personal Information	High: This information is inherent to the company and can be used against them if revealed.
Equipment	Medium: This equipment might potentially hold personal information, but it is highly unlikely if it is plugged out. It can also easily be replaced at a cost to the university.
Building/Surroundings (Wi-Fi etc.)	Medium/High: These assets can be easily replaced by the university if damaged.

3 Threats and Exposures Research

3.1 External Malicious Attacks

External malicious attacks are the most common attacks that affect systems and organizations that operate like The Pluto University. External attackers tend to use social engineering techniques to exploit “human error to gain private information, access, or valuables”, luring users into “exposing data, spreading malware infections, or giving access to restricted systems” (Kaspersky, 2020). In order to appeal to a large audience and to yield the best return on time investment, a large percentage of social engineering attacks in university systems are carried out using phishing; these attackers try to impersonate a “trusted institution or individual in an attempt to persuade users to expose personal data and other valuables” (Kaspersky, 2020). Email phishing attacks are more common throughout universities due to their ability to be distributed quickly and vastly without much effort and interaction with the targeted victims. These attacks are also some of the most effective as they bank on the victim not paying enough attention to the phishing email in order to work and yield a high success rate.

3.2 Ransomware Attacks

Another common threat posed to modern university systems revolve around ransomware attacks. Crackers know that universities make large amounts of money every single year, and even during the current situation regarding the pandemic, UK universities have still managed to charge normal prices for higher education to almost “2.38 million students” (HSEA, 2019). Ransomware cyber-attacks involve the act of upgrading the phishing and social engineering practices by not only stealing/compromising the organization’s data, but also “demanding payment for the recovery of this frozen or stolen data” (BBC, 2020) via a ransom note, hence the name. These types of attacks are aimed at bigger and more established organizations as they yield a better chance of enticing the victim to pay them the sum that they are asking for. As of July 2020, more than “20 universities and charities in the UK, US and Canada had confirmed they were victims of a cyber-attack that compromised a software supplier” (BBC, 2020). This shows that this is still a very relevant threat to be on the lookout for, as even in uncertain times, it still plagues universities and organizations like The Pluto University.

3.3 Internal non-malicious attacks

The unfortunate truth is that the biggest security threat to a system is the very people that work within/benefit from the system. When speaking about a university system, the two main factors that contribute to this problem are the students that use the system, and the staff that provide services to the students. Students are the more reckless of the two groups of people, as students can unknowingly expose an entire system to threats by visiting unsafe websites, downloading dodgy documents, and compromise their own data by simple acts like leaving their computer's unattended while in public. However, employees of these given organizations are not always the most qualified, careful and/or mindful when handling potentially sensitive aspects of their employment agencies either; the majority of data breaches can be directly attributed to employee behaviours such as an "inability to follow policies and procedures" (Frangiskatos, 2019). The repercussions for minor dips in concentration like this can be catastrophic, with some including but not limited to: "millions of personal records being compromised, a plethora of government investigations, heavy fines and sanctions, reputational damage and the media baying for blood" (Frangiskatos, 2019). In order to prevent this, institutions such as The Pluto University should make sure to educate stakeholders as to how they can keep themselves and their data secure. All parts of the system must be "aware of their responsibilities with regards to the guardianship of data" (Frangiskatos, 2019).

3.4 Internal malicious attacks

The least common of all the researched topics, there is always a possibility that an employee or student will intentionally attack the given system. Once again, both students and employees are subject to this kind of behaviour, with no real distinction between the both of them in this regard. Consumers of organizations like The Pluto University are likely to intentionally harm the university for reasons such as them being disgruntled, unhappy and/or having "hatefulness for other consumers or the service providers" (Yadav et al., 2016). Internal stakeholders might also want to show "the company a weakness in their security" as well as to get "revenge or glory" (Frangiskatos, 2019). Employees and students will also tend to possess a smaller skill set that hackers/crackers etc., so they will tend to use "less sophisticated attack methods" such as "stealing confidential information through

online tools or USB drives” (Shackleton, 2020).

4 Risk Assessment and Risk Treatment Strategy

Based on the research conducted, and with reference to the material studied in the COMP1608 module; a decision was made to use a combination of international IT governance standard models and risk assessment matrices in order to determine the appropriate risk assessment and management strategies. These were then to be analysed and documented in the well-designed tables shown below for ease of access. ISO 27001 and 27005 are used for risk identification and management tasks respectively. The risk assessment matrix is used to aid in the risk identification task as well. Examples of all three models are shown in the index (chapter 8):

4.1 Risk Identification (ISO 27005)

Risk/Threat	Description	Risk Type	Affects	Origin
External malicious attacks	Social engineering, phishing scams etc.	Compromise of information (tampering with software) Technical failures (breach of information system)	Employees Students System Owners	Deliberate
Ransomware attacks	Demanding ransom whilst carrying out malicious attacks	Compromise of information (tampering with software) Unauthorized actions (illegal processing of data)	Employees Students System Finances	Deliberate
Internal non-malicious attacks	Internal stakeholders inadvertently putting the system at risk	Compromise of functions (error in use)	Employees Students System	Accidental

Internal malicious attacks	Internal stakeholders purposefully putting the system at risk	Unauthorized actions (illegal processing of data) Compromise of functions (Breach of personnel)	Employees Students System	Deliberate

4.2 Risk Analysis and Matrices (ISO 27005):

Risk	**Likelihood**	**Business Impact**	**Rank on Matrices Table**
External malicious attacks	Medium	High	5
Ransomware attacks	Medium	High	5
Internal non-malicious attacks	Medium	Medium	4
Internal malicious attacks	Low	High	4

4.3 Risk Management Strategy (ISO 27001):

Shown below is an example of the four risk management strategies, and how they could possibly affect the decision-making regarding threats, risk and security.

Risk	**Strategy**			
	Avoidance	**Transfer**	**Mitigation**	**Acceptance**
External malicious attacks	Implement a system that nullifies the possibility of an attack	Transfer risk to a 3rd party security company	Implement a system that notifies the IS of an attack	Accept the possibility of an attack happening regardless

Ransomware attacks	Implement a system that nullifies the possibility of an attack	Transfer risk to a 3rd party security company	Implement a system that notifies the IS of an attack	Accept the possibility of an attack happening regardless
Internal non-malicious attacks	Make sure to vet and teach all stakeholders how to avoid accidental mistakes (creating strong passwords etc.)	Transfer the task of teaching these skills to a 3rd party security company/online course	Implement a system that warns a stakeholder of potentially dangerous actions	Accept the possibility of an attack happening regardless
Internal malicious attacks	Give special security access to absolutely no one	Transfer the task of managing the IT system to a trusted 3rd party company	Only give special security access to trusted stakeholders	Accept the possibility of an attack happening regardless

5 Introducing New Technology to the Operations

The proposed change in the Pluto University system involves a system update in the software used in the IT department; this is a realistic change as real-life IT systems often have to update their systems to adapt to changing requirements.

5.1 Impact on existing risk analysis and management system

Introducing new hardware or software to an already existing system is never an easy task. In addition to the already existing stakeholders in the current system, new additions to information systems often include new technology related: hardware, software, data, people and processes. In addition to this, the ever-changing nature of IT means that there will always be accidental issues that are caused by the internal stakeholders such as employees while trying to upscale a system. However, as Fred Brooks' highlights in his 1987 paper 'No Silver Bullet', these changes also bring along a string of essential difficulties that are inherent to software development as a whole. These four essential difficulties are "complexity, conformity, changeability and invisibility" (Brooks, 1987).

The essential issues that are most relevant in this scenario in regard to Brooks' study revolve around conformity and changeability; the system's ability to conform to new standards and requirements and its ability to adapt to the changing nature of IT as mentioned before. The new addition to the information system must be able to conform to the old features of the system without causing issues including but not limited to loss of data, integration issues, file corruption and system failure. Another issue that has to be taken into consideration, has nothing to do with the hardware or software of the process, but more to do with the legal, social, ethical and professional implications (LSPEi) of upscaling the system. Failure to account for any of these issues can result in issues that can cost the system a large amount of money, time and humiliation to repair. To avoid unnecessary waffle/repetitiveness, only the most important and noticeable changes in the risk management process have been documented, as many of the risks that can affect both the old and new system are similar.

Potential New Stakeholders	Roles/Impact
Business Partners	Setting financial constraints, maximizing returns on security spending, introducing new software companies and experts
Staff	Learning new system, shaking up hierarchy to fit new system guidelines, teaching new staff to use system effectively, working with new security staff
Students	Learning to use new system, new technology attracts more/wider variety of students as more needs can be accommodated

5.2 Revised Risk Analysis and Matrices (ISO 27005):

Risk	Likelihood (compared to first analysis)	Business Impact	Rank on Matrices Table
External malicious attacks	Medium: Stays the same, the risk will always exist	High	5
Ransomware attacks	Medium: Stays the same, the risk will always exist	High	5
Internal non-malicious attacks	Low: There's a lower chance a internal stakeholders knowing the new system completely	Medium	3
Internal malicious attacks	Very High: There's a higher chance of users not knowing how to completely use the new system.	High	7

6 Conclusion

The importance of an Information Systems Management System cannot be downplayed at all. Having the given system implemented helps to ensure that the system's services, information and stakeholders are secure, and the risks are identified and managed correctly. These tasks are not only the responsibility of the system. It is up to humans themselves to make sure that they are aware of the IT risks that they face every day, and by choosing secure passwords, following rules, and staying safe online, they create an environment that is much safer for them online as the platform continues to change.

7 References

- Brooks (1987) No Silver Bullet Essence and Accidents of Software Engineering, *Computer*, 20(4), pp. 10-19.

- Coughlan, S. (2020) Cyber threat to disrupt start of university term, *BBC News*, [online] Available at: https://www.bbc.co.uk/news/education-54182398 (Accessed 23 December 2020).

- HSEA (2020) Higher education in numbers, *Universitiesuk.ac.uk*, [online] Available at: https://www.universitiesuk.ac.uk/facts-and-stats/Pages/higher-education-data.aspx (Accessed 23 December 2020).

- Kaspersky (2020) What is Social Engineering?, *www.kaspersky.co.uk*, [online] Available at: https://www.kaspersky.co.uk/resource-center/definitions/what-is-social-engineering (Accessed 23 December 2020).

- Lee, J. (2020) Security Threats Facing Universities, *Infosecurity Magazine*, [online] Available at: https://www.infosecurity-magazine.com/opinions/security-threats-universities/ (Accessed 23 December 2020).

- S. A. Yadav, S. R. Kumar, S. Sharma and A. Singh, "A review of possibilities and solutions of cyber attacks in smart grids," *2016 International Conference on Innovation and Challenges in Cyber Security (ICICCS-INBUSH)*, Noida, 2016, pp. 60-63, doi: 10.1109/ICICCS.2016.7542359.

- Schoenhard, L. (2019) 4 Ways Stakeholders are Important to a Project | Proficient Learning, *Proficient Learning*, [online] Available at: https://proficientlearning.com/4-ways-stakeholders-are-important-to-a-project/ (Accessed 23 December 2020).

- Tidy, J. (2020) Blackbaud hack: More UK universities confirm breach, *BBC News*, [online] Available at: https://www.bbc.co.uk/news/technology-53528329 (Accessed 23 December 2020).

8 Appendix

8.1 ISO 27005, ISO27001 and Risk Assessment Matrix

… and ISO 27005

- (A) Accidental, (D) Deliberate, (E) Environmental

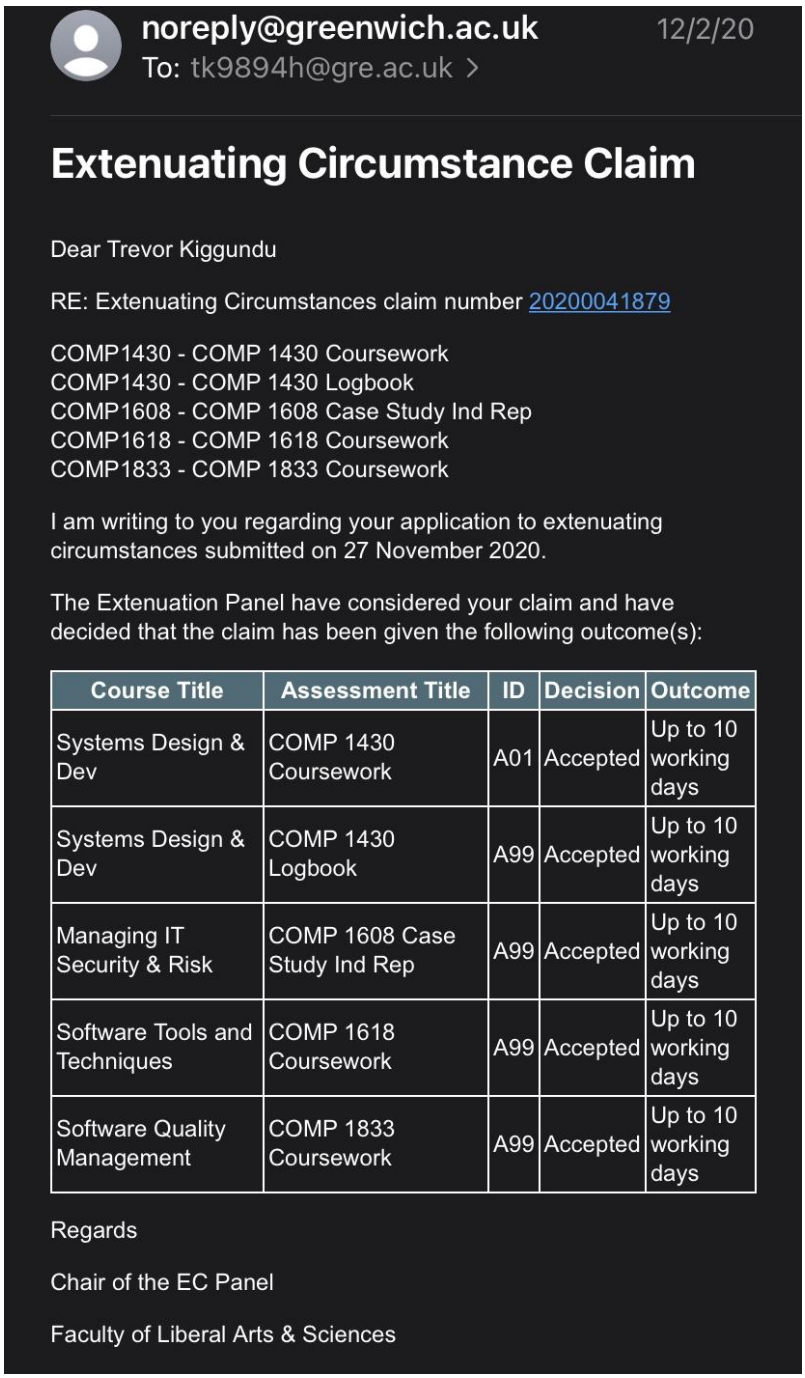
Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E

Type	Threats	Origin
Technical failures	Equipment failure	A
	Equipment malfunction	A
	Saturation of the information system	A, D
	Software malfunction	A
	Breach of information system maintainability	A, D
Unauthorised actions	Unauthorised use of equipment	D
	Fraudulent copying of software	D
	Use of counterfeit or copied software	A, D
	Corruption of data	D
	Illegal processing of data	D
Compromise of functions	Error in use	A
	Abuse of rights	A, D
	Forging of rights	D
	Denial of actions	D
	Breach of personnel availability	A, D, E

Type	Threats	Origin
Physical damage	Fire	A, D, E
	Water damage	A, D, E
	Pollution	A, D, E
	Major accident	A, D, E
	Destruction of equipment or media	A, D, E
	Dust, corrosion, freezing	A, D, E
Natural events	Climatic phenomenon	E
	Seismic phenomenon	E
	Volcanic phenomenon	E
	Meteorological phenomenon	E
	Flood	E
Loss of essential services	Failure of air-conditioning or water supply system	A, D
	Loss of power supply	A, D, E
	Failure of telecommunication equipment	A, D
Disturbance due to radiation	Electromagnetic radiation	A, D, E
	Thermal radiation	A, D, E
	Electromagnetic pulses	A, D, E
Compromise of information	Interception of compromising interference signals	D
	Remote spying	D
	Eavesdropping	D
	Theft of media or documents	D
	Theft of equipment	D
	Retrieval of recycled or discarded media	D
	Disclosure	A, D
	Data from untrustworthy sources	A, D
	Tampering with hardware	D
	Tampering with software	A, D
	Position detection	D

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

8.2 Approved Extenuating Circumstances Claim



noreply@greenwich.ac.uk 12/2/20
To: tk9894h@gre.ac.uk >

Extenuating Circumstance Claim

Dear Trevor Kiggundu

RE: Extenuating Circumstances claim number 20200041879

COMP1430 - COMP 1430 Coursework
COMP1430 - COMP 1430 Logbook
COMP1608 - COMP 1608 Case Study Ind Rep
COMP1618 - COMP 1618 Coursework
COMP1833 - COMP 1833 Coursework

I am writing to you regarding your application to extenuating circumstances submitted on 27 November 2020.

The Extenuation Panel have considered your claim and have decided that the claim has been given the following outcome(s):

Course Title	Assessment Title	ID	Decision	Outcome
Systems Design & Dev	COMP 1430 Coursework	A01	Accepted	Up to 10 working days
Systems Design & Dev	COMP 1430 Logbook	A99	Accepted	Up to 10 working days
Managing IT Security & Risk	COMP 1608 Case Study Ind Rep	A99	Accepted	Up to 10 working days
Software Tools and Techniques	COMP 1618 Coursework	A99	Accepted	Up to 10 working days
Software Quality Management	COMP 1833 Coursework	A99	Accepted	Up to 10 working days

Regards

Chair of the EC Panel

Faculty of Liberal Arts & Sciences