2024

IT & Cybersecurity Governance, Policy, Ethics and Law

ASSIGNMENT 1B

JOPHIEL AREVALO ENRIQUEZ

EXECUTIVE SUMMARY

This report aims to provide an in-depth and comprehensive analysis of IT & Cybersecurity Governance, Policy, Ethics and Laws. These principles help companies how to organize manage and protect their information systems and data. Establishing these policies and laws ensure the secure operation of every IT system while maintaining legal and ethical standards. These four components ensure that organizations approach IT and cybersecurity in a responsible and lawful manner so this way companies can mitigate risks and promote trust between organizations and their stakeholders.

The report is structured in 10 different modules which analyze each topic in a comprehensive way, where the topic is developed according to the delimitations established for a better understanding of them. Each theme has an objective of fusion between examples and theoretical and practical research topics that are aligned with current trends in the IT industry. The following is a brief recap of each module.

MODULE 1

This module analyses the IT governance frameworks such as COBIT or ITIL, their benefits, advantages and qualities for an optimal implementation to reach industry standards and provides a roadmap for a successful implementation.

MODULE 2

This module develops the idea and the implementation of a hacking policy, taking into account the objectives, roles and responsibilities that the policy should have. This module tries to exemplify by means of a practical-theoretical analysis where the procedures of such a policy are prioritized.

MODULE 3

In an IT environment it is essential to have a plan for a possible data breach, this module explains in detail how to develop such a plan, the responsibilities and procedures that the people involved should follow to maintain a standard and eliminate risks due to lack of knowledge within the processes of a plan.

MODULE 4

Using an example of a hospital (Zenith) this module tries to explain incident management by prioritizing and justifying the capabilities (Prepare, Protect, Detect, Respond, Sustain) that the hospital has, giving a projection to improve the situation in phases.

MODULE 5

This module analyses an ethical dilemma involving a human resources IA system that biasedly selects candidates for a company, lists the main ethical issues and recommends possible solutions for this type of problem.

MODULE 6

This module provides an analysis of the ethical implications of open-source software licensing; it also provides a more practical view of what open-source software licensing is, examples of misuse and how it benefits the evolution of technology.

MODULE 7

This module explains the process of forensics and threat intelligence, its research and development (Readiness, Evaluation, Collection, Analysis, Presentation, Review), how to improve the cyberthreat program, its benefits and objectives.

MODULE 8

This module deals with ethical and inclusive technology for social good, intensifying a current social problem which is intolerance to the LGBTQ community, how new technologies help this problem, giving a perspective and an ethical solution with the people involved.

MODULE 9

This module helps to understand the implications and controls of cybersecurity in the face of attacks such as malware, how to react and how to act in these situations, and how insurance companies are becoming more and more powerful with new technologies.

MODULE 10

This module addresses the new trends in remote working and how companies should react, knowing that the development of specific policies on remote working will help to ensure the privacy and security of employees and employers.

TABLE OF CONTENTS

MODULE 1: EVALUATING IT GOVERNANCE FRAMEWORKS 6

IT Framework Management Plan 6
Introduction 6
Frameworks benefits and challenges 6
ITIL 6
COBIT 6
Roadmap 7
Conclusion 7
References 7

MODULE 2: DEVELOPING AN ETHICAL HACKING POLICY 9

Ethical Hacking Policy 9
Introduction 9
Scope 9
Objectives 9
Roles and responsabilities 9
Guidelines and reporting 10
Confidentiality and legal awarness 10
Conclusion 10
References 10

MODULE 3: DATA BREACH RESPONSE PLAN 12

Cybertech Data Breach Response Plan 12
Introduction 12
Key roles 12
Plan 12
Contain 12
Assesment 13
Notify 13
Review 13
Conclusion 13
References 14

MODULE 4: ASSESSING INCIDENT MANAGEMENT MATURITY 15

Zenith Incident Management Maturity 15
Introduction 15
Maturity model/Capabilities 15
Roadmap for improvement 16
Conclusion 17
References 17

MODULE 5: ETHICAL AI CASE STUDY ANALYSIS 18

TechnoCore Ethical Dilemma 18
Introduction 18
Ethical issues 18
Legal risks 18
Discrimination 18
Transparency 18

Equity 18
Ethical use of AI: 18
Prioritzation of ethical problems *19*
Recomendations *19*
Conclusion *19*
References *19*

MODULE 6: THE ETHICS OF OPEN-SOURCE SOFTWARE LICENSING 21

OSS ETHICAL IMPLICATIONS 21
Introduction *21*
Ethical considerations *21*
Open-Source Software license 21
Mitigating risks 22
Conclusion *22*
References *22*

MODULE 7: CYBER FORENSICS AND INTELLIGENCE ANALYSIS 23

THREAT INTELLIGENCE AND FORENSICS 23
Introduction *23*
Cyber forensics Investigation Process *23*
Readiness 23
Evaluation 23
Collection 23
Analysis 23
Presentation 23
Review 23
Threat analysis *24*
Technical intelligence (TECHINT) 24
Signal Intelligence (SIGINT) 24
Open-source Intelligence (OSINT) 24
Cyberthreat Intelligence Program *24*
Conclusion *24*
References *25*

MODULE 8: ETHICAL AND INCLUSIVE TECHNOLOGY FOR SOCIAL GOOD 26

LGBTQ COMMUNITY INTOLERANCE 26
Introduction *26*
Desired social impact *26*
Ethical principles and standards *26*
Accessibility and Inclusivity *26*
Stakeholder Engagement *27*
Ethical decision-making *27*
Accountability *27*
Conclusion *27*
References *27*

MODULE 9: ASSESSING CYBER RISK AND INSURANCE NEEDS 29

RANSOMWARE ATTACKS 29
Introduction *29*
Risk and potential impacts *29*
Cybersecurity controls *29*

Cybersecurity Insurance *30*
Conclusion *30*
References *30*

MODULE 10: BALANCING PRIVACY AND SECURITY IN REMOTE WORK POLICIES 32

REMOTE WORK REVOLUTION 32
Introduction *32*
Data Security Measures *32*
Monitoring and Surveillance Practices *32*
Handling and Sharing Sentitive Information *32*
Acceptable Use of personal devices and public networks *32*
Training and awareness program *33*
Compliance with relevant laws and regulations *33*
Balancing Organizational needs with individual privacy *33*
Conclusion *33*
References *33*

MODULE 1: EVALUATING IT GOVERNANCE FRAMEWORKS

IT FRAMEWORK MANAGEMENT PLAN

INTRODUCTION

This report aims to evaluate and analyse the IT governance frameworks the company currently has. The company is going through a time where customers doubt the IT attention provided. In addition, there have been several security and compliance incidents. This is why a self-evaluation, and recommendations are required to improve the management and oversight of the company's IT resources and processes.

FRAMEWORKS BENEFITS AND CHALLENGES

IT governance frameworks provide essential rules and guidelines for organizations to manage their IT resources and processes effectively (Tuffley, 2023). Given the case of a medium-sized company with financial data where there are IT problems, it is important to mention that there is no specific recommendation for a single framework since, we can mix some and extract the best of each related to the company.

ITIL

One of the problems established in the company is customer complaints related to its IT operations; we can begin by proposing a solution within the theoretical framework of ITIL. The IT Service Management (ITSM) which involves designing, delivering, managing, and improving IT services to meet the needs of customers and stakeholders (IBM, n.d.). This is beneficial for the company since by applying a specific system, it is expected to have benefits such as improvements in customer-company relationships, service quality, cost reduction, and resource optimization are essential strategies in service management, alongside the implementation of effective IT service actions and supporting digital transformation aligned with the business goals (Atlassian, n.d.).

COBIT

Another factor to consider is a comprehensive evaluation of security and compliance due to the problems that the company has been presenting such as security incidents and compliance issues. COBIT align I&T goals with business objectives, optimizing I&T resources and processes, and ensuring effective control and assurance over I&T activities are essential for designing, implementing, monitoring, evaluating, and improving internal controls (ISACA, 2016). This is why this framework is aligned with the needs that the company is going through and by following the guide it provides, the control system for problems such as security incidents can be solved and improved. For example, by controlling the company's internal system, practical solutions can be strengthened, and feedback can be

obtained from past problems for the correct control of these. Therefore, customer loyalty and trust.

The most important challenge is the implementation of each of the elements, comply with all the frameworks. Also, considering that it is a medium-sized company and can be adjusted to the specific needs that the company has.

ROADMAP

For a correct implementation Tuffley (2023) suggest:

- Determine the IT compliance standards relevant to your business. This involves the company analysing the applicable regulations in the financial sector, such as the Sarbanes-Oxley Act (SOX) for financial reporting, the Gramm-Leach-Bliley Act (GLBA) for protecting financial data, or the Payment Card Industry Data Security Standard (PCI DSS).
- Evaluate your current compliance status. The best approach for the company is to engage an external audit service to accurately identify any existing issues.
- Implement the necessary security measures to meet compliance standards. This requires the adoption of frameworks like COBIT.
- Regularly monitor and maintain your compliance status. After evaluation and implementation, ongoing monitoring is essential to uphold quality standards and stay aligned with the latest industry developments.

CONCLUSION

Taking into account the above, it is expected to carry out an exhaustive analysis of the current situation of the company, with a framework such as COBIT that will help the company improve internal processes to solve security and compliance problems and implementing the practices that the ITIL framework has to raise the service that the company has towards its clients to a higher level through a roadmap that specifies the steps to follow with critical activities and established quality levels.

REFERENCES

Atlassian. (n.d.). What is ITIL? A guide to ITIL 4 framework. https://www.atlassian.com/itsm/itil

IBM. (n.d.). What is IT Infrastructure Library (ITIL)?. What Is IT Infrastructure Library (ITIL)? | IBM

ISACA. (2016). Essential frameworks and methodologies to maximize the value of IT. ISACA Journal, 2. https://www.isaca.org/resources/isaca-journal/issues/2016/volume-2/essential-frameworks-and-methodologies-to-maximize-the-value-of-it

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes.* Griffith University.

MODULE 2: DEVELOPING AN ETHICAL HACKING POLICY

ETHICAL HACKING POLICY

INTRODUCTION

According to Palmer (2001) an ethical hack aims to test the system in the way an intruder would do but without malicious intentions, that means, an ethical hacker must have the same skills as a malicious person but for the benefit of the system or the company.

Within the company we are analysing, a system needs to be evaluated to see the possible implications that a large financial company may have in the event of a possible hack of the system.

SCOPE

The ethical hacking program has a preventive scope, this means that the program will conclude as the program evolves, in other words, this program is designed to end when there is a minimum favourable result of penetration into the system, thus being the least invasive for it, protecting the sensitive data handled within the company.

OBJECTIVES

- Test the current system with sophisticated hacking techniques to analyse its operation and reaction to this.
- Implement preventive actions for massive hacks by educating the business community with the possible effects of a leak in the system.
- Relate potential hacks to real cases to create an action plan for possible future cases.

ROLES AND RESPONSABILITIES

Ethical hacking necessitates not only advanced technical skills but also a strong adherence to ethical standards and legal compliance to ensure responsible and authorized actions (Syed, 2006). This is why in a company of such magnitude, a team must be considered that handles and understands all the implications that an ethical hack entails, considering that the data is sensitive:

- Ethical hackers should focus on identifying vulnerabilities through penetration tests and offering solutions to enhance security (Sinha & Arora, 2006).
- Ethical hackers must adhere to legal and ethical standards, ensuring transparency and confidentiality in their work (Syed, 2006).

- Ethical hacking teams not only identify vulnerabilities but also support incident response and enhance cybersecurity strategies (Sinha & Arora, 2006).

GUIDELINES AND REPORTING

There are some steps to follow for implementation within the company:

- When dealing with extremely sensitive data that involves government laws, specific data from large clients due to the nature of the company, it is advisable and experts such as Tuffley (2023) assure that the consent should be documented in writing, with a detailed plan outlining the steps to be taken to breach the system.
- Next, within the testing phase, current techniques that involve common hacking activities must be handled. It is crucial to collect and document every step taken, along with the reasoning behind each action, when managing a program of this scale (Tuffley, 2023).
- Finally, Tuffley (2023) recommends that insert quote from the book, a report should be made with all the findings of the program that specifies all the actions taken with their due justification, conclusions and legal, technical or educational recommendations for the system.

CONFIDENTIALITY AND LEGAL AWARNESS

As a financial company with a large client portfolio where sensitive economic data from various other institutions, client accounts and critical information are handled daily, confidentiality must be handled according to the best standards, which is why the company must align these indicators with the CIA model, a foundational concept in cybersecurity, emphasizes that data access should be limited to authorized personnel, ensuring the integrity and availability of data are maintained (Irwin, 2023)

CONCLUSION

In conclusion, ethical hacking, as Tuffley (2023) said, can benefit organizations in various ways, such as improving their security posture, enhancing their reputation, complying with regulations, and saving costs, but it must follow a series of procedures to be effective. The company must follow the ethical hacking procedures having in mind the sensitivity of financial data, we must work with professionals with responsible skills, aware of the magnitude of what is involved in an ethical hack.

REFERENCES

C. C. Palmer, "Ethical hacking," in *IBM Systems Journal*, vol. 40, no. 3, pp. 769-780, 2001, https://doi.org/10.1147/sj.403.0769

Irwin, L. (2023). *What is the CIA triad and why is it important?* IT Governance. https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

Sinha, S & Arora, Y. (2006) Ethical Hacking:The Story of a White Hat Hacker. *International Journal of Innovative Research in Computer Science & Technology (IJIRCST),* ISSN: 2347-5552, Volume-8, Issue-3. http://dx.doi.org/10.2139/ssrn.3670801

Syed A. S. (2006). Ethical hacking as a risk management technique. *In Proceedings of the 3rd annual conference on Information security curriculum development (InfoSecCD '06).* 201–203. https://doi.org/10.1145/1231047.1231089

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes.* Griffith University.

MODULE 3: DATA BREACH RESPONSE PLAN

CYBERTECH DATA BREACH RESPONSE PLAN

INTRODUCTION

There are numerous techniques developed for unauthorized data acquisition, known as data breaches. As these breaches have evolved, companies must be vigilant about adhering to regulations and understanding the procedures to follow when such incidents occur. (Molitor et al., 2023). This is why CyberTech has developed the following plan for Data breach, below are the main aspects to follow for this type of eventuality.

KEY ROLES

The plan must be limited to specific roles which together make a joint contribution to be able to act in an efficient and effective manner in any data breach situation, because the company has a record of sensitive data, has access to employee data and even its main activity is focused on obtaining data or reinforcing security levels for companies.

This is why Tuffley (2023) suggest the following roles:

- Team leader, responsible for the team and its operation
- Project manager, responsible for coordination
- Senior staff, expert responsible for technical issues
- Legal support, expert responsible for legal issues
- Risk manager support, responsible for breach risks
- Forensics, responsible for investigations ◦ HR support, responsible for the human aspect involved in the company
- Media experts, responsible for notifications and communications inside and outside the company

PLAN

The 4 steps to follow within a data breach plan are the following:

CONTAIN

After a data breach has been identified, the first critical step is to contain it. Immediate actions are necessary to control the breach, which involves understanding its origins, implementing measures to stop its spread, and minimizing further damage. (OAIC, 2023)

Cybertech team should:

- Change the data access authorization, revoke privileges

- the senior staff should work among the manager to reduce all the risks and try to contain it with the best strategies.
- Identify the possible reasons for the data breach
- Try to work with copies of the disks, ensure that there are no more external people involved and start an assessment to see the possible damages

ASSESMENT

OAIC, (2023) recommended that the next step is to create an assessment to ensure the risks of the breach.

Cyber tech team should:

- Reformulate the events with all possible details, people involved, circumstances and magnitude of the breach
- Evaluate all the data obtained to be able to formulate them in a precise manner
- Magnify the weight of the breach in order to be able to continue with a specific notification to the entities involved

NOTIFY

If the risk is significant or there remains a potential threat, it is crucial to notify the relevant entities and individuals involved. Under the NDB scheme, this notification must be made to the OAIC and may also be published in the media with necessary explanations of the case. (OAIC, 2023)

Cybertech team should:

- Explain preventive actions that those involved must take to secure the exposed data must be handled.
- Determine whether notification to all parties involved is necessary or only to specific entities depending on the case.

While notification is being made, Tuffley (2023) state that the handling of any questions that arise from the individuals must be considered; the reaction of the team to those involved is fundamental for an engagement with them.

REVIEW

Finally, after the containment, analysis and notification processes, the incident should be thoroughly reviewed so that actions can be taken for future conflicts or leaks. According to OAIC, (2023) relevant non-direct entities should be notified.

CONCLUSION

In conclusion, CyberTech's data breach plan must be fully implemented, respecting the parameters established in the plan, formulating the best and most effective solutions with the people best prepared for this type of eventuality, and following the recommendations under the legal and jurisdictional terms of each case.

REFERENCES

Molitor, D., Raghupathi, W., Saharia, A., & Raghupathi, V. (2023). Exploring key issues in cybersecurity data breaches: Analyzing data breach litigation with ML-based text analytics. *Information, 14*(11), 600. https://doi.org/10.3390/info14110600

Office of the Australian Information Commissioner (OAIC). (2023). Notifiable Data Breaches Report: January to June 2023. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes.* Griffith University.

MODULE 4: ASSESSING INCIDENT MANAGEMENT MATURITY

ZENITH INCIDENT MANAGEMENT MATURITY

INTRODUCTION

The most critical and sensitive points that Zenith must address to counteract the current IT problems, taking into account that it processes sensitive patient data on a daily basis and that it cannot stop operations due to a leak are (Table 1 is presented which expresses a list of capability statements contained in the SEI-CMU's cybersecurity Maturity Model from which the critical points have been extracted according to the case (Stewart & Hoover, 2020), they are necessary and a priority). In the context of Zenith, where they do not have specific plans or previous knowledge, it is important to emphasize priorities I.

MATURITY MODEL/CAPABILITIES

According to Tuffley (2023) the capabilities to focus are:

Capability	Priority	Maturity level	Justification
Prepare			
Roles and responsibilities are documented for key incident management.	I	Managed	Considering the current situation of zenith where there are no protocols to follow.
An incident management plan has been developed and implemented.	I	Basic	There is no plan to follow if any incident were to happen, zenith employees have no idea of the recommendations to follow.
An insider threat program exists.	I	Basic	Zenith does not have an internal incident control system; the IT department priority is to have an internal preparation plan since now none is presented.
Protect			
Security risk assessments (RAs) are performed.	I	Mature	It is necessary to have a risk assessment to protect and know the risks that an incident can cause to Zenith Hospital.
The organization has an institutionalized malware prevention program.	I	Basic	The knowledge and prevention of the hospital staff is scarce, a prevention and awareness program must be created for all employees.
Detect			
Security monitoring is continuously performed.	I	Defined	IT department must ensure constant control of networks and systems since when handling health data,

Penetration testing is conducted.	I	Defined	It is known that the procedures are empirical and there is no strict plan to follow.
Respond			
Events and incidents are reported from the constituency.	I	Basic	Zenith has a lack in the identification of these, which is why staff training is a priority.
Incident analysis is performed on declared incidents.	I	Basic	Zenith must have an exhaustive analysis for the incidents that may occur and be reported due to its high inability to react to any event.
Incident management personnel coordinate incident response across stakeholders.	I	Basic	There is no deep knowledge of the risks and implications that incidents can cause.
Sustain			
Formal agreements exist for managing IM activities with third parties across the supply chain.	I	Basic	There must be agreements between the parties in the supply chain since each one handles data in a different way.
A training program exists for incident management personnel.	I	Basic	Zenith must have an established plan since now there is no type of training for non-IT personnel.
Defence-in-depth strategies and methodologies exist for hardening the incident management.	I	Managed	Zenith does not have a structured plan to follow. In addition, actions and responsibilities must be limited.

ROADMAP FOR IMPROVEMENT

Phase 1: Immediate Actions

• Deploy advanced threat detection tools, such as Qradar SIEM. (IBM, n.d.)

• Conduct cybersecurity awareness sessions focusing on phishing and social engineering tactics.

Phase 2: Short-term Actions

• Organize incident response drills to test the effectiveness of the coordination protocols and make necessary adjustments based on outcomes.

• Develop comprehensive recovery plans that include data restoration, system recovery, and continuity strategies for critical medical services.

Phase 3: Long-term Actions

• Conduct regular reviews and updates of all incident management plans, ensuring they remain effective against current threats.

CONCLUSION

Maras (2021) aim that focusing on critical capabilities like incident identification, response coordination, recovery, security awareness, and incident analysis, can significantly enhance its cybersecurity posture. Zenith Hospital will protect sensitive patient data, ensure business continuity, and safeguard the hospital's reputation and trust in its services

REFERENCES

IBM. (n.d.). *Advanced Threat Detection - QRadar SIEM*. https://www.ibm.com/products/qradar-siem/advanced-threat-detection

Maras, M.-H. (2021). *Cybersecurity: Incident Response*. In Encyclopedia of Security and Emergency Management. Springer. https://doi.org/10.1007/978-3-319-70488-3_301

Stewart, K. C., & Hoover, A. F. (2020, March 30). *An introduction to the Cybersecurity Maturity Model Certification (CMMC)*. Software Engineering Institute, Carnegie Mellon University. https://insights.sei.cmu.edu/blog/an-introduction-to-the-cybersecurity-maturity-model-certification-cmmc/

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes.* Griffith University.

MODULE 5: ETHICAL AI CASE STUDY ANALYSIS

TECHNOCORE ETHICAL DILEMMA

INTRODUCTION

TechnoCore has some ethical dilemmas that must be analyzed by the implementation of the new AI system that helps in the hiring of new staff. The critical aspects that the company must prioritize are impartiality and fairness throughout the hiring process (Dattner et al., 2019). This report highlights the aspects to consider for a comprehensive evaluation of the system.

ETHICAL ISSUES

LEGAL RISKS

The use of an educated system to select a certain group of individuals leads to legal problems where the balance is not balanced, the company can face problems of discrimination and unfair hiring practices. The reputation that the company manages is also put at stake, losing credibility in the market (MehaffyWeber, 2023).

DISCRIMINATION

Due to the system having a biased training, the results thrown by the AI system had a certain affinity for people with special characteristics, without considering all the applicants. This results in discrimination putting certain candidates at an unfair disadvantage compared to others (Manyika et al., 2019).

TRANSPARENCY

By using a biased model, many candidates will think that there is no transparency for each case, this in turn will generate uncertainty among the people who are going through the hiring process (Manyika et al., 2019).

EQUITY

There has not been equity and equal conditions when selecting the optimal candidate, this means that several candidates who are not within the bias framework do not have the same opportunities as others and are still capable of all the conditions set out for said job (Manyika et al., 2019).

ETHICAL USE OF AI:

The ethical implications that a machine can have must be addressed, senior management must ensure that the use of this technology is integral, transparent and ethical. For this, there are several frameworks such as those suggested by the EEOC for optimization and monitoring of clear rules by companies in the use of these new technologies (MehaffyWeber, 2023).

PRIORITZATION OF ETHICAL PROBLEMS

• Legal risks: a thorough examination of all legal implications must be made, and these must be aligned with the use of new technologies.

• Equity: Ensure equal treatment for all candidates even if this is a higher cost for the company since when configured in a biased way, the AI system is not being as fair and objective as possible.

• Bias: The elimination of any type of bias is essential to have equal treatment in any process that the company requires.

RECOMENDATIONS

The immediate suspension of the service provided by AI is essential in this case since the implications of continuing to use such a system can be disastrous for the company itself. In addition, create and analyze the configurations which were initially biased, eliminate them to prevent legal and reputational risks (Wade, 2024).

Maintain constant audits where possible bias within the AI system is tested, this type of audits can be carried out by external companies for greater objectivity in the case.

Have a person who supervises and has the final decision over the AI system which can capture this type of bias and intervene in any type of impartial result.

CONCLUSION

The use of AI in a hiring process opens a world of possibilities, however, the ethical implications that this can have must be considered since if it is not correctly configured it can create an unequal system for all candidates (Manyika et al., 2019). TechnoCore must reevaluate the system, regardless of the costs that this entails since the consequences of continuing to use this unethical system can be devastating. It is recommended to follow the relevant protocols that companies and legal organizations must follow, this problem has not only been imposed on TechnoCore, Tuffley (2023) in his book mentions a list of prestigious institutions that recommend protocols to follow with the use of AI.

REFERENCES

MehaffyWeber. (2023, April 10) *Can using AI in hiring practices result in a lawsuit?* (2023). https://www.mehaffyweber.com/news/can-using-ai-in-hiring-practices-open-your-business-up-to-a-discrimination-lawsuit/

Dattner, B., Chamorro-Premuzic, T., Buchband, R., & Schettler, L. (2019). *The legal and ethical implications of using AI in hiring. Harvard Business Review.* https://hbr.org/2019/04/the-legal-and-ethical-implications-of-using-ai-in-hiring

Manyika, J., Silberg, J., & Presten, B. (2019). *What do we do about the biases in AI?* Harvard Business Review. https://hbr.org/2019/10/what-do-we-do-about-the-biases-in-ai

Tuffley, D. (2023). 7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes. Griffith University.

Wade, C. (2024). Navigating the ethical and legal risks of AI implementation. CIO. https://www.cio.com/article/2149672/navigating-the-ethical-and-legal-risks-of-ai-implementation.html

MODULE 6: THE ETHICS OF OPEN-SOURCE SOFTWARE LICENSING

OSS ETHICAL IMPLICATIONS

INTRODUCTION

This report aims to identify and analyse the ethical implications that a developer who has created a powerful data analysis tool using various Open-source software libraries must have and must find the best option to use. This alternative must be justified, and finally, the measures to mitigate the ethical risks that are compatible with the interests of the stakeholders will be mentioned.

To begin, we must keep in mind the definition of Open-source software. For this, David (2023) suggests that open-source software is a program that allows other users to investigate it and, if the purposes of this are beneficial to the person who needs it, the free license allows it to be used, modified or changed. In other words, the OSS allows programmers to freely use and distribute their source code.

ETHICAL CONSIDERATIONS

99% of 1000 applications analysed have some open-source component. This makes open-source software a fundamental pillar for software development today (Bernhard, 2021). Therefore, it is important to know the ethical implications that this should entail. Today there are several licenses that developers can work with. However, the definition of freedom can vary according to the interpretation that is given to it.

The analysis the Centre for Applied Ethics (n.d.) provides us with a utilitarian perspective in the face of an ethical dilemma is clear when mentioning whether the human being can handle all access to information in the same way. This is why some ethical considerations must be raised for the proposed topic as it is a data analysis tool that can harm people.

One of the ethical considerations is the misuse of open-source software. Bernhard (2021) in his publication mentions a clear example where the US Air Force declares to have a percentage of open-source software in its fleet of F-16 warplanes. This implies that due to its definition, OSS can be used for military purposes.

OPEN-SOURCE SOFTWARE LICENSE

Tuffley (2023) mentions in his book that there are two types of licenses that dictate the terms and conditions of Open-source software, the first, permissive, being the one that gives the most permission to the creators to modify the code under the same name of the main author and the copyleft that forces the modifiers to share their modifications.

In this case, the best option, given the background that the developed tool could cause some kind of damage, is copyleft since it provides in a certain way a better control over the modifications that the software is having, according to the Free Software Foundation (n.d.) in order to create or modify a program, you must have access to all the versions that it has.

MITIGATING RISKS

Ethical licenses can also be considered, as Bernhard (2021) mentions in his article, the Hippocratic license created by Coraline Ada Ehmke in 2019 would mitigate risks for the software because it places ethical restrictions on the use of Open-source software. However, these measures have not been fully accepted since the OSI (Open-Source Initiative) has different contrasts since this concept violates the principle of an open license which dictates that software can be freely used by anyone (Tuffley, 2023).

CONCLUSION

A developer must consider the ethical implications of each case, Copyleft is a tool to control the operation of software, in this case the publication of modifications or the use of the software will allow the creator to ensure its use. Nowadays there are several types of licenses that can help us mitigate some risks. However, these measures are not yet fully accepted since they contradict the principles of Open-source software.

REFERENCES

Bernhard, M. (2021). *Open-source software: Freedom from ethics?.* Engineering & Technology, vol. 16, no. 4, pp. 1-9. IEEE Xplore Full-Text PDF:

Center for Applied Ethics. (n.d.). *Unavoidable ethical questions about open source.* Markkula Center for Applied Ethics, Santa Clara University. Unavoidable Ethical Questions About Open Source - Markkula Center for Applied Ethics (scu.edu)

Free Software Foundation. (n.d.). *What is Copyleft?.* GNU Operating System. https://www.gnu.org/licenses/copyleft.en.html\

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes*. Griffith University.

MODULE 7: CYBER FORENSICS AND INTELLIGENCE ANALYSIS

THREAT INTELLIGENCE AND FORENSICS

INTRODUCTION

This report aims to conduct a cyber forensics investigation and gather threat intelligence to understand the nature of the breach and the potential actors involved. Since the company has recently experienced a data breach.

CYBER FORENSICS INVESTIGATION PROCESS

The discipline of forensics in cybersecurity is a key process to determine some key events in investigations or even to stop or mitigate processes that may occur (Tuffley ,2023), this process must be methodical and that is why the following steps must be considered:

READINESS

According to Tuffley (2023) within this process the people who will be involved in the investigation process must be considered. In our case, there must be a competent team that knows the procedures to follow in the event of a data breach.

EVALUATION

The evaluation of the investigation is key since here all the implications that it has are developed and under what parameters it must be worked (Tuffley, 2023). In our case, the legal aspects of data manipulation.

COLLECTION

IBM (n.d.) mentions that the integrity of the collected data must be ensured. In our case, exact and precise copies of the disks where the data breach occurred must be made.

ANALYSIS

To facilitate the analysis, ERMProject (2021) mentions that this process must be methodically and objectively carried out to identify the exact causes of the incident. In our case, this is where the causes of the data breach can be collected.

PRESENTATION

IBM (n.d.) suggests that this process be precise to reach the standards that a court requires. In our case, a comprehensive report must be created with clear and concise evidence, with neutral language that is understandable to anyone.

REVIEW

This process has nuances of self-assessment to identify lessons and control in the future. For our case, here we will analyse the consequences and causes to reinforce security for future occasions (ERMProject, 2021).

THREAT ANALYSIS

For this case, the following sources of cyber intelligence have been collected:

TECHNICAL INTELLIGENCE (TECHINT)

Van Impe (2023) mentions in its article that this type of intelligence helps to collect information from the equipment, which is why it is helpful to analyse the technical capabilities of the equipment in a data breach.

SIGNAL INTELLIGENCE (SIGINT)

According to Maltego (2023), this type of intelligence analyses communications between devices, which is why it would be very helpful to see what happened between the communications of a possible data breach.

OPEN-SOURCE INTELLIGENCE (OSINT)

Van Impe (2023) announces that this intelligence helps to verify through various open means the strategies for a data breach, with this type of intelligence the latest modalities of the people and how they are carrying out said strategies can be verified.

CYBERTHREAT INTELLIGENCE PROGRAM

Following Impe's recommendations in its article, the program established for cyber intelligence must have varied components.

To start, Van Impe (2023) recommends getting a successful team, people who are experts in various subjects and have knowledge of incident response. Also, within the first stages, Van Impe (2023) recommends having a rigorous data collection process.

The strategic components must affirm clear and precise objectives, and the creation of policies for proper operation is essential.

Having external collaborators also gives a different perspective for a successful program (Van Impe, 2023), which is why collaborating with different entities such as ISAC is an appropriate step.

CONCLUSION

Having an adequate program with established controls within cyber forensics helps with the immediate response to events such as data breaches, collaborating between entities, and having a robust team that is aware of the technical and legal implications is essential for a successful team.

REFERENCES

ERMProtect. (2021, June 21). *What are the 5 stages of a digital forensics investigation?* ERMProtect. https://ermprotect.com/blog/what-are-the-5-stages-of-a-digital-forensics-investigation/

IBM. (n.d.). *What is computer forensics?*. IBM. https://www.ibm.com/topics/computer-forensics

Maltego. (2023, February 22). *Understanding the different types of intelligence collection disciplines*. Maltego. https://www.maltego.com/blog/understanding-the-different-types-of-intelligence-collection-disciplines/

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes.* Griffith University.

Van Impe, K. (2023, February 10). *What are the different types of cyberthreat intelligence?* Security Intelligence. https://securityintelligence.com/what-are-the-different-types-of-cyberthreat-intelligence/

MODULE 8: ETHICAL AND INCLUSIVE TECHNOLOGY FOR SOCIAL GOOD

LGBTQ COMMUNITY INTOLERANCE

INTRODUCTION

According to Electronic Frontier Foundation (2023) many countries have increased intolerance towards the LGBTQ community. This is why LGBTQ-Mobile proposes the creation of a digital platform where users can be free to express themselves, as well as the possibility of having free psychological help from members of the same community.

Knight (2024) analyses the impact of developed countries such as Germany having new police forces that benefit this community; however, this trend is not universal, and many other countries are rejecting them outright. The goal of LGBTQ-Mobile is to generate a platform where users feel safe and can educate themselves or have support from the same community.

DESIRED SOCIAL IMPACT

The impact that this platform wants to have is to generate an integrated adaptation of users that empowers users and teaches them their rights and the strength that this community has. In addition, it is desired to have legal advice for people and promote education and equality in the community.

ETHICAL PRINCIPLES AND STANDARDS

Among the ethical principles of a platform that defends mistreatment of the LGBTQ community are equity where all people must be treated equally even within the platform, this also refers to the fact that if a person does not identify with the community, they can also access the platform. In addition, transparency and privacy of all people involved in the process must be ensured. Finally, accountability and inclusivity to ensure its proper functioning and non-discrimination regardless of gender identity.

ACCESSIBILITY AND INCLUSIVITY

The platform is designed as a safe space for the community, where knowledge of rights and social help within it are reinforced by professionals who also share and better understand each situation. For this reason, Tuflley (2023) suggests also promoting the dissemination of these offline spaces for the inclusion of people who may not have digital resources but want to be part of it. LGBTQ Mobile prioritizes the inclusion of languages, cultures and specific content for each geographic area. Tuffley (2023) also suggests having innovative features like text to speech or even sign language videos.

STAKEHOLDER ENGAGEMENT

Key Stakeholders: LGBTQ+ individuals, families, allies, NGOs, advocacy groups, technology providers, and government bodies.

Feedback Loops: Regularly collect and act on feedback from users and stakeholders.

Advisory Committees: Establish committees with representatives from key stakeholder groups.

ETHICAL DECISION-MAKING

For clear ethical decision-making, the respect and openness that the community itself aims for must always be considered; the platform and all its decisions must always be fair, without discrimination or prejudice.

ACCOUNTABILITY

Reporting on ethical considerations must be fair and accurate as well as being regular. Younes (2024) in his publication writes about the digital discrimination that many people in this community suffer daily, especially in African or Middle Eastern countries, which is why LGBTQ-Mobile also opens the doors to people with a privacy method where it not only ensures their well-being but makes it much more manageable for this type of case. The union of the community in workshops that connect with users to educate them and make them aware of their rights and vulnerabilities in order to reinforce their strengths. The platform must always be controlled and evaluated for its correct operation where it aligns with the proposed guidelines.

CONCLUSION

LGBTQ-Mobile is an emerging technology that is not only a social platform, it is the link with this community, where users can have confidence and at the same time be educated and aware of all the support that this community gives them, in addition, focusing not only on the virtual aspect LGBTQ-Mobile wants to be a pioneer in the development and fight against the threats that they themselves have experienced in these times.

REFERENCES

Electronic Frontier Foundation. (2023, December 30). *International threats to freedom of expression.* https://www.eff.org/deeplinks/2023/12/international-threats-freedom-expression-2023-year-review

Knight k. (2024). *When laws fail to protect trans people, harmful medicalized norms creep in.* https://www.hrw.org/news/2024/05/15/when-laws-fail-protect-trans-people-harmful-medicalized-norms-creep

Tuffley, D. (2023). 7*907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes.* Griffith University.

Younes R. (2024*). Treacherous internet: Cyber-criminalization of LGBT people.* https://www.hrw.org/news/2024/06/12/treacherous-internet-cyber-criminalization-lgbt-people

MODULE 9: ASSESSING CYBER RISK AND INSURANCE NEEDS

RANSOMWARE ATTACKS

INTRODUCTION

The following report aims to analyse the consequences of a malware attack on a medium-sized manufacturing company. As part of the cybersecurity team, it is essential to consider the causes and processes to follow so this type of cyber threats cannot continue to spread. It is also essential to know the risks that these can generate in the company, specifically ransomwares that aim to extort and try to receive high amounts of money in exchange for the release of data.

RISK AND POTENTIAL IMPACTS

Tuffley (2023) explains in his book the risks that contagious malware can cause to a company. This type of malicious software uses a penetration strategy to the devices or networks of a system.

One of the main malwares that has gained strength in recent times is Ransomware, which reaches sensitive data in a system and restricts access to it until a payment is made by the owner Cisco (n.d.).

The potential impacts that ransomware could have on a manufacturing company could be disastrous. Depending on how compromised the system is, the ransomware or hacker behind it may ask for a high sum of money for the release of the content. Even payment would not ensure the return or non-manipulation of the data. In addition, while this occurs, the cessation of operations by the company would mean a substantial loss of production (Federal Bureau of Investigation, n.d.).

CYBERSECURITY CONTROLS

IBM (2024) explains in its article the methodology that this type of malware takes from the moment of infection where the most common initialization attacks are phishing, vulnerability exploitation and compromising remote access protocols like RDP until its exposure, because it is a malware that acts quickly, the controls that must be taken are preventive.

The Federal Bureau of Investigation (n.d.) recommends on its page to have up-to-date backups, also constantly updating the devices and their operating systems since these have patches that help protect the device against this type of attacks, create a security plan to prevent these attacks, and make sure all the antivirus and antimalware are up to date scanning all the devices regularly.

Decentralizing the departments within the manufacturing company is a good strategy to prevent these attacks, in addition to making weekly backups with

sensitive content, having backups in clouds or even auditing and securing the company against these types of threats are fundamental tools to prevent these risks. Community education through tests or simulations is a strategy for mitigating this type of malware.

CYBERSECURITY INSURANCE

The impact and growth that cyber insurance is having in everyday life only reflects the tendency of companies to digitize their systems, this has many benefits and is noticeable in the trends, but it is also accompanied by several challenges that time ago were not considered for companies Tuffley (2023). Therefore, from small companies to giant companies are beginning to invest in this type of security, Al-rimy, Maarof, & Shaid. (2018) Comment in their article on the evolution of this type of insurance and its rapid growth in various sectors. For this reason, mitigating residual risks with insurance is an effective strategy to control the company's exposure to cyber threats.

CONCLUSION

In recent times, malware has evolved largely due to the growth in the digital world. One of the many is ransomware, which encrypts sensitive data on a system and expects payment in exchange for its release. As a medium-sized manufacturing company, it is important to consider preventive controls so that this type of malware does not directly affect it. There must be prevention campaigns, backups, constant operating system updates, cloud backups, and contract insurance services to mitigate residual risks.

REFERENCES

Al-rimy, B. A. S., Maarof, M. A., & Shaid, S. Z. M. (2018). *Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions*. Computer Science Review, 32, 67–87. https://doi.org/10.1016/j.cosrev.2017.01.001

Cisco. (n.d.). *What is malware?*. Cisco. https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html

Federal Bureau of Investigation. (n.d.). *Ransomware*. FBI. https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/ransomware

IBM. (2024, June 4). *What is ransomware?*. IBM. https://www.ibm.com/topics/ransomware

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes*. Griffith University.

MODULE 10: BALANCING PRIVACY AND SECURITY IN REMOTE WORK POLICIES

REMOTE WORK REVOLUTION

INTRODUCTION

While it is true that remote work has revolutionized the way many employees and employers view a job, some recommendations must be taken for the common good. It is essential for a large company or government agency to set clear and concise recommendations and guide to monitor and maintain real and fruitful business objectives (Tuffley, 2023).

DATA SECURITY MEASURES

Regarding data security measures, Gertenbach (2024) recommends implementing basic cybersecurity hygiene, basic controls such as keeping software up to date or constantly scanning the device. He also recommends using a VPN or using multi-factor authentication to access sensitive data. Employee privacy rights and consent

Tuffley (2023) recommends that employers should build a work environment based on trust, where employee privacy prevails above all else, it should be aligned with privacy principles such as the Australian Privacy principles, where employee consent must be obtained to monitor activities, trying to avoid any type of discriminatory treatment or that is against the principles mentioned above.

MONITORING AND SURVEILLANCE PRACTICES

The practices that an employer must follow regarding the surveillance of remote workers must be seen in terms of achievements (Forbes, 2021). The recommendation at this point is to set clear objectives since various challenges are faced such as working hours, communication tools, or cultural differences. For this reason, policies must be proposed where effective communication prevails in which the employer measures the results of remote employees in an optimal way.

HANDLING AND SHARING SENTITIVE INFORMATION

Mitigate this risk by providing employees with company-owned tools that are for business use only, thus reducing the risk of data leaks. Forbes (2021) in its article emphasizes the creation of a robust business policy in which security is prioritized and has established security protocols. Here, the use of encrypted tools or the use of cloud tools that help with constant data monitoring can also be emphasized.

ACCEPTABLE USE OF PERSONAL DEVICES AND PUBLIC NETWORKS

Ensure employee training and awareness when using devices for personal purposes, try to mitigate the use of public networks and raise awareness of how to

handle data within this type of network, try not to use unsafe sites for a work environment.

TRAINING AND AWARENESS PROGRAM

Maintaining constant training for all remote employees is essential since by raising awareness of the consequences and controlling the measures, a deeper environment of trust can be generated. Therefore, this continuous training guide that may have simulations of potential breaches or malware is excellent for continuity in a remote environment (Gertenbach, 2024).

COMPLIANCE WITH RELEVANT LAWS AND REGULATIONS

Workers must consider the laws and regulations that the company must ensure before any stakeholder, the remote worker must consider and follow the privacy recommendations no matter where they are, it is important to emphasize that remote work has obligations and rights as much as working on site (Tuffley, 2023).

BALANCING ORGANIZATIONAL NEEDS WITH INDIVIDUAL PRIVACY

Tuffley (2023) also mentions the benefits that this type of work has for both the employer and the employee, however, it is important to clarify that the policies must be clear since there will be uncertainties on the part of both at the time of working, therefore, the balance that must exist must be measured in different ways, the privacy and performance of employees is closely linked to the control policies that the employer needs to have to evaluate business objectives.

CONCLUSION

Having a robust policy for remote work is essential for any company, constantly ensuring good practices for good performance and continuous training is essential for a relationship between employee and employer to work. But above all, there must be an environment of trust between both parties where communication prevails and there are incentives and achievements on the part of both.

REFERENCES

Forbes Technology Council. (2021, October 14). *15 strategies for securing company data in a remote workplace*. Forbes. https://www.forbes.com/sites/forbestechcouncil/2021/10/14/15-strategies-for-securing-company-data-in-a-remote-workplace/

Gertenbach, E. (2024). *Data security best practices: Top 10 tips for remote teams*. Upwork. Top 10 Data Security Practices for Remote Work | Upwork

Tuffley, D. (2023). *7907ICT IT & Cybersecurity Governance, Policy, Ethics & Law: Course Notes*. Griffith University.