7907ICT IT & CYBERSECURITY GOVERNANCE, POLICY, ETHICS AND LAW

ASSIGNMENT 1A

SHEHRYAR MALLICK

S5328488

shehryar.mallick@griffithuni.edu.au

CONTENTS

MODULE 1: EVALUATING IT GOVERNANCE FRAMEWORKS 2

Introduction 2
Purpose And Scope 2
Governance Framework 2
Compliance Requirements 3
Monitoring And Reporting 3
Roles And Responsibilities 3
Conclusion 4
References 4

MODULE 2: DEVELOPING AN ETHICAL HACKING POLICY 5

Introduction 5
Scope And Objective Of Ethical Hacking Program 5
Roles And Responsibilites Of The Ethical Hacking Team And Other Stakeholders 5
Obtaining Consent And Authorization 6
Guidelines, Tools, And Techniques For Ethical Hacking Program 6
Reporting And Communication Procedures 6
Measures To Protect Sensitive Data And Maintain Confidentiality 6
Mechanism For Monitoring And Auditing Ethical Hacking Activities 7
Procedures For Addressing Legal And Regulatory Compliance Requirements 7
The Provisions For Training And Awareness Programs On Ethical Hacking Practices 7
The Strategies For Mitigating Legal And Reputational Risks Associated With Ethical Hacking 7
Conclusion 8
References 8

MODULE 3: DATA BREACH RESPONSE PLAN 9

Introduction 9
Key Roles And Responsibilities 9
Data Breach Response Plan 10
Notify Related Parties 11
Conclusion 11
References 11

MODULE 4: ASSESSING INCIDENT MANAGEMENT MATURITY 12

Introduction 12
Prioritized Incident Management Capabilities 12
Current Maturity Model 14
Proposed Road Map 15
Conclusion 15
References 15

MODULE 5: ETHICAL AI CASE STUDY ANALYSIS 17

Introduction 17
Key Ethical Issues Identified 17
Prioritization Of Issues Based On Ethical Principles: 17
Recommended Solution And Rationale For Ethical Justification 18
Conclusion 18
References 19

MODULE 1: EVALUATING IT GOVERNANCE FRAMEWORKS

Optimizing IT Governance with COBIT and ITIL Strategies

INTRODUCTION

The issue at hand necessitates an IT governance framework to address security breaches, legal non-compliance, and unmet customer expectations. This document outlines a comprehensive approach to developing such a framework, focusing on the essential factors of Structure, Process, and Communication (Symons, 2005). It is created from the perspective of a Chief Information Security Officer (CISO) and considers the organization's role as a financial institution. The framework ensures adherence to data privacy standards and compliance with state laws applicable to both the organization's location and its clients' jurisdictions

PURPOSE AND SCOPE

The scope of the problem can be divided into three aspects Security, Compliance and Stakeholder Expectations. The objective of the framework is to focus on improving the management of the company and in turn dealing with individual aspect while at the same time providing a monitoring mechanism to assess the effectiveness of the proposed framework.

GOVERNANCE FRAMEWORK

To address our IT governance challenges, we have selected COBIT and ITIL frameworks. COBIT is chosen for its comprehensive coverage of IT governance, spanning strategy to operations, with four domains and 37 control objectives. These cover planning, organization, acquisition, implementation, delivery, support, and monitoring, aligning with our financial firm’s needs (Tuffley, 2023; Symons, 2005). Key COBIT objectives include risk assessment, IT procedures management, system accreditation, and compliance, making it highly relevant for our scope.

Security: Assess risk, manage project, Develop and maintain IT procedures, Install and accredit system, ensure system security, manage problems and incidents, monitor process, provide for independent audits.

Compliance: Ensure compliance, Communicate aim and direction, manage data. Customer

Compliant: Manage quality, Manage performance and capacity, assist and advise IT customers. These objectives belong to the 4 domains discussed earlier and each play a vital role in the establishment of the framework to tackle the problem (Symons, 2005; Hurkadli, 2023).

We selected ITIL for its emphasis on delivering high-quality products and services to stakeholders and customers. Relevant ITIL aspects include:
Improving customer satisfaction, enhancing IT services, reducing costs, and supporting digital transformation. Improve customer satisfaction, Enhance IT services, Reduce costs and risks, Increase agility and innovation, Support digital transformation (Tuffley, 2023)

COMPLIANCE REQUIREMENTS

The framework cannot stand on its own and needs support of the relevant regulatory and legal requirement, the selection criteria is based on the fact we are a financial firm, have accumulated sensitive customer data, and are operating in different regions.

Based on the stated factors the relevant compliance standards include: The General Data Protection Regulation (GDPR) to ensure the protection of customer data, and The Payment Card Industry Data Security Standard (PCI DSS) to protect the credit/debit card info of the customer (Tuffley, 2023). Other compliance policies include: The Sarbanes-Oxley Act (SOX), which focuses on the protection of storage and management of financial records, and finally 23 NYCRR 500 which is a set of cybersecurity regulations that ensure that financial institutions protect their systems and customer data against cyber-attacks (Wolf, 2023).

MONITORING AND REPORTING

A framework and policies are ineffective without a monitoring and reporting method to assess performance and adapt as needed. Board performance is significantly influenced by reporting quality (Kaawaase et al., 2021). After implementing the framework and policies, we can use the seven guiding principles of ITIL to guide decisions and actions. Key steps include establishing a

Service Management Office (SMO),

Monitoring and measuring service performance,

Reporting and communicating achievements,

Reviewing and evaluating outcomes and feedback,

Identifying and prioritizing improvement initiatives,

Implementing improvements using methods like the PDCA cycle (plan-do-check-act).

ROLES AND RESPONSIBILITIES

Chief Information Security Officer (CISO): Oversees IT governance framework.

Service Management Office (SMO): Manages service performance.

Board: Reviews and adapts based on reporting quality.

CONCLUSION

The IT governance framework, leveraging COBIT and ITIL, addresses security, compliance, and stakeholder satisfaction. By defining clear roles, adhering to regulatory standards, and implementing robust monitoring and reporting mechanisms, the framework ensures effective management and continuous improvement, safeguarding both organizational integrity and customer trust.

REFERENCES

Hurkadli, R. (2023, August 30). COBIT Controls list XLS. ITSM Docs.https://www.itsm-docs.com/en-au/blogs/cobit/cobit-controls-list-xls

Kaawaase, T. K., Nairuba, C., Akankunda, B., & Bananuka, J. (2021). Corporate governance, internal audit quality and financial reporting quality of financial institutions. Asian Journal of Accounting Research, 6(3), 348-366.

Symons, C. (2005). IT governance framework. Forrester research.

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

Wolf, A. (2023, July 28). The Top Compliance Regulations for Financial Institutions. Arctic Wolf. https://arcticwolf.com/resources/blog/a-simplified-regulatory-checklist-for-financial-institutions/

MODULE 2: DEVELOPING AN ETHICAL HACKING POLICY

Ethical Hacking A Need of Modern Cyber Threats

INTRODUCTION

As the Chief Information Security Officer of a major financial institution, you face the challenge of implementing an ethical hacking program while navigating legal risks and upholding ethical standards.

SCOPE AND OBJECTIVE OF ETHICAL HACKING PROGRAM

To effectively define the scope and objectives of the ethical hacking program, follow these steps:

Identify the Target: The main goal is to improve the company's cybersecurity. Objectives include pinpointing vulnerable assets, forming a cyber team for penetration testing, setting up a compliance team for industry standards, deploying a SIEM solution for ongoing monitoring, notifying stakeholders, and ensuring regulatory compliance to avoid legal issues.

Define Boundaries: Establish clear boundaries to avoid any corruption of internal data during penetration testing.

Identify Critical Assets: Focus on client data (personal, account, credit/debit information), employee data (personal information, physical IDs), transaction and financial systems, APIs in core infrastructure, data warehouses, analytics systems, and IT infrastructure (workstations, network devices, cloud services).

Determine Protection Level and Allocate Resources: Prioritize assets, assess risks, set deadlines, and allocate resources to start the program.

This approach ensures a comprehensive and strategic setup for the ethical hacking program. (Gtcsys Technology Partners, n.d.).

ROLES AND RESPONSIBILITES OF THE ETHICAL HACKING TEAM AND OTHER STAKEHOLDERS

1. Clients: Notify clients about the program through a disclaimer, ensuring data protection. Clients should review the privacy notice and have the option to opt out if the program doesn't align with their values.
2. CISO: Ensure the program complies with state laws, industry standards, and procedures while overseeing and delegating team duties.
3. Ethical Hacking and Compliance Team: Conduct penetration testing in a controlled environment and develop mitigation and recovery procedures.
4. Employees: Inform employees about the program and provide relevant cybersecurity training to protect assets.

5. Executive Team: Approve the program, allocate resources, and determine the acceptable risk level.

OBTAINING CONSENT AND AUTHORIZATION

Consent and authorization involve three key parties:

1. **Employees and Management:** Notify employees through training and obtain explicit written permission from executives.
2. **Government:** Ensure compliance with government laws, and in case of a breach, notify authorities under the Notifiable Data Breaches scheme (Australian Government, n.d.).
3. **Customers:** Obtain customer consent via a voluntary, informed, specific, and current consent form to proceed with the ethical hacking program (Queensland Government, 2023; Morin, 2023).

GUIDELINES, TOOLS, AND TECHNIQUES FOR ETHICAL HACKING PROGRAM

1. The following guidelines are essential for developing an effective plan:

2. Obtain written consent from all relevant parties to conduct testing.

3. Create a sandbox environment to ensure real customer data remains unaffected in case of issues (Any Run, 2024).

4. Ethical hackers should mimic techniques used by black-hat hackers to identify and document system vulnerabilities (Palmer, 2001; Jena, 2024).

5. Base testing approaches on established cybersecurity frameworks like the Penetration Testing Execution Standard (PTES).

6. Utilize industry-standard tools such as Nmap, Metasploit, and Nessus.

7. Define clear boundaries to prevent disruption to daily operations, networks, or systems.

REPORTING AND COMMUNICATION PROCEDURES

An initial report should detail assets, risk levels, and penetration testing techniques. After testing, submit findings and recommendations. Post-implementation, provide a performance report and periodic executive updates for ongoing monitoring and threat management.

MEASURES TO PROTECT SENSITIVE DATA AND MAINTAIN CONFIDENTIALITY

To protect sensitive data, implement the CIA triad principles: ensure confidentiality by restricting access to authorized users (Fortinet, n.d.), enforce

access control privileges (Microsoft, n.d.), and comply with the Privacy Act of 1998 to prevent misuse of customer data (Australian Government, n.d.).

MECHANISM FOR MONITORING AND AUDITING ETHICAL HACKING ACTIVITIES

Monitor ethical hacking activities with real-time reports detailing discoveries, techniques, and recommendations weekly. Additionally, create audit trails that document the tools used, results obtained, and threats identified in a systematic manner to ensure comprehensive oversight and transparency throughout the process.

PROCEDURES FOR ADDRESSING LEGAL AND REGULATORY COMPLIANCE REQUIREMENTS

The notable compliance and legal requirement can be fulfilled using the following frameworks:

1. Privacy act 1998
2. Notifiable Data Breaches (NDB) scheme
3. Penetration Testing Execution Standard (PTES)
4. NIST

THE PROVISIONS FOR TRAINING AND AWARENESS PROGRAMS ON ETHICAL HACKING PRACTICES

The first step involves training employees with regular sessions on security protocols, common errors, and best practices. The executive team will also be educated on industry standards, the ethical hacking program's importance, and vulnerability management.

THE STRATEGIES FOR MITIGATING LEGAL AND REPUTATIONAL RISKS ASSOCIATED WITH ETHICAL HACKING

1. Notify both the government and clients of any breaches under the Notifiable Data Breaches (NDB) scheme.
2. Maintain transparency with clients about the ethical hacking program's goals and obtain their consent.
3. Ensure NDAs are signed by all hacking and compliance team members to protect data after they leave.
4. Develop an incident response plan to address and mitigate any attacks.

CONCLUSION

Implementing these guidelines ensures ethical hacking programs are conducted transparently, with proper consent, data protection, and incident management, enhancing system security and compliance

REFERENCES

(n.d.). How do you define the scope of a cybersecurity project? Gtcsys Technology Partners. https://gtcsys.com/faq/how-do-you-define-the-scope-of-a-cybersecurity-project/

Queensland Government (2023, November 16). Obtaining and managing student and individual consent procedure. https://gtcsys.com/faq/how-do-you-define-the-scope-of-a-cybersecurity-project/

Morin, M. N. (2023, March 30). What You Need to Know About Customer Consent in 2023. https://www.dialoginsight.com/en/blog/security-and-conformity/customer-consent/

Australian Government (n.d.). About the Notifiable Data Breaches scheme. https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

Palmer, C. C. (2001). Ethical hacking. IBM Systems Journal, 40(3), 769-780.

(2024, February 20). How to Create a Sandbox Environment (for Malware Analysis). Any Run. https://any.run/cybersecurity-blog/how-to-create-a-sandbox/

Jena, B. K. (2024, August 13). What is Ethical Hacking? A Comprehensive Guide [Updated]. Simplilearn. https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-ethical-hacking#

(n.d.). What is the CIA Triad? Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad#

(n.d.). What is access control? Microsoft. https://www.microsoft.com/en-au/security/business/security-101/what-is-access-control

(n.d.). Privacy. Australian Government. https://www.ag.gov.au/rights-and-protections/privacy#

MODULE 3: DATA BREACH RESPONSE PLAN

CyberTech Data Breach Response Plan

INTRODUCTION

Assuming the role of CyberTech's CISO, this document outlines a data breach response plan. It details key team members' responsibilities, the step-by-step response process, and the notification procedures for relevant parties. The plan is tailored to a medium-sized company with a turnover exceeding $3 million.

KEY ROLES AND RESPONSIBILITIES

Following are the associated roles in a data breach response team (Australian Government, n.d.; Federal Court of Australia, 2020):

Team Leader: The team leader is responsible for overseeing the breach response, assessing its severity, and taking appropriate actions. They delegate tasks, ensure the response team understands their roles, and debrief them on the incident. The team leader is also responsible for notifying senior management and associated parties.

Legal Support: Legal support plays a crucial role in the response team. They assess the legal implications of the breach and advise the team on how to proceed in accordance with state laws and regulations. They ensure that all actions taken are legally sound and protect the organization from potential legal repercussions.

Risk Management Support: Risk management support involves analysing the potential risks caused by the breach. This includes identifying affected parties, assessing vulnerable systems or assets, and determining the harm posed to individuals whose data has been compromised (Information Commissioner Office,2023).

Information and Communication Technology (ICT)/Forensics Support: The ICT team investigates the cause of the breach, identifies specific system vulnerabilities, and works to mitigate the breach. They create incident reports to ensure future prevention and provide recommendations for securing the system. They also assess controls such as access rights, system authentication, and encryption algorithms.

Human Resources (HR) Support: HR support is essential in handling internal personnel issues, particularly if an employee is responsible for the breach. They also arrange training sessions between the response/cyber team and other employees to ensure staff is adequately trained in cybersecurity.

Media/Communications Expertise: This team is responsible for crafting the official response to notify customers and clients. They also draft the response for government notifications under the Notifiable Data Breaches (NDB) scheme.

DATA BREACH RESPONSE PLAN

The response plan has the following four crucial steps with sub-steps on how to effectively implement each step(Australian Government, n.d.; Security Metrics, n.d.; NSW Government n.d.):

Step 1: Contain:

- Notify the response team promptly.
- Identify the breached data, affected parties, and vulnerable systems, noting the time and date of the breach.
- Disconnect from the internet to stop data leakage and close affected applications.
- Disable remote access, document old passwords, and change them immediately.
- Preserve firewall settings, firewall logs, system logs, and security logs.
- Restrict internet traffic so only critical business servers operate while quarantining the rest of the network.

Step 2: Assess

- Identify the type of data involved and whether it can uniquely identify individuals, triggering a confidentiality breach that requires notification.
- Determine the system's weaknesses, the breach's scope, and duration.
- Assess any financial implications, such as loss of customer credit information or risks to customer health.

Step 3: Notify

- Determine if the breach meets the requirements of the NDB scheme (Australian Government, n.d.) and notify the government if necessary.
- Notify clients whose data was compromised, advising them to change passwords, and maintain trust through transparency.
- Report to senior management, the executive board, and third-party partners to allow them to assess their systems.
- Notify the insurer for additional support.

Step 4: Review

- Conduct a security review to identify the breach's root cause and test containment and mitigation measures.
- Check other vulnerable system parts and develop mitigation strategies.
- Implement audits to ensure the prevention plan's effectiveness.
- Debrief the team and employees on the breach for future prevention.
- Assess third-party partners' compliance with industry standards.

NOTIFY RELATED PARTIES

In case of a breach, notify the following:

Clients: Issue a legal notice via email, assuring mitigation.

Employees: Debrief on the incident and train on breach response.

Executive Team: Inform about the breach, potential loss, and mitigation steps.

Government: Notify OAIC per the NDB scheme requirements (Australian Government, n.d.).

CONCLUSION

In conclusion, this comprehensive data breach response plan equips CyberTech with the necessary strategies to swiftly and effectively manage incidents, ensuring minimal disruption and maintaining trust with clients, employees, and stakeholders.

REFERENCES

Australian Government (n.d.). Part 2: Preparing a data breach response plan. Australian Government Office of the Australian Information Commissioner. https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response/part-2-preparing-a-data-breach-response-plan

Federal Court of Australia (2020, July 31). Data Breach Response Plan. https://www.fedcourt.gov.au/privacy/data-breach-response-plan

Information Commissioner Office (2023, August 30). Understanding and assessing risk in personal data breaches. ICO. https://ico.org.uk/for-organisations/advice-for-small-organisations/understanding-and-assessing-risk-in-personal-data-breaches/

Security Metrics (n.d.). How to Effectively Manage a Data Breach. https://www.securitymetrics.com/learn/how-to-effectively-manage-a-data-breach

NSW Government (n.d.). Data Breach Response Plan. Data.NSW. https://data.nsw.gov.au/sites/default/files/inline-files/Data%20Breach%20Response%20Plan.pdf

Australian Government (n.d.). About the Notifiable Data Breaches scheme. Australian Government Office of the Australian Information Commissioner. https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

MODULE 4: ASSESSING INCIDENT MANAGEMENT MATURITY

Zenith Hospital: A step into incident management

INTRODUCTION

About Organization: The organization that we are to work on is Zenith Hospital which is a medical care centre.

Current Standing: Has only basic response procedures in-place.

Evident Vulnerabilities:

Phishing attack on staff

No evident compliance policy and protection technique implemented to protect customer data.

No policy implemented for business continuity and real time mitigation.

In-adequate staff training that can lead to exploitation.

Task assigned:

The first task is the assessment of current cyber security structure.

Utilization of SEI incident management model to introduce improvements, prioritize capabilities more closely aligned to healthcare.

Development of incident management plan with a focus on three vital aspects identification, communication and recovery.

Introduction to improvement roadmap.

PRIORITIZED INCIDENT MANAGEMENT CAPABILITIES

In-order to have a robust model implemented we have selected the following capabilities to deal with the organizational vulnerabilities that are closely aligned to health care. The capabilities are based on SEI-CMU cyber security model, we have developed a table for better understanding with the following key attributes and their description (Tuffley, n.d.):

Area - Defines one of the five main domain of incident management.

Capability - Is the actual capability that the incident management plan should have and to be implemented by the organization.

Priority - The priority level assigned to the capability.

Justification - support for using the specific capability in the incident management plan.

Capability	Area	Priority	Justification
1.1.1 An incident management function or CSIRT has been officially designated by the organization head or chief information officer (CIO).	Prepare	2	For any organization irrespective of the area they operate in, the need for a single reliable point of contact that specifically deal with computer security incidents and who also deals with the incident related information, recovery, assessment, and development is crucial (Nduhiu, 2023).
1.1.2 An incident management plan has been developed and implemented for the organization.	Prepare	1	Some of the key benefits for the development and implementation of an incident response plan include (Atlassian, n.d.): • Effective and timely recovery of the affected system • Communicate the incident to all affected parties • Collaborative effort with designated roles defined to respond. • Continuous improvement.
1.2.5 A central repository exists for recording and tracking security events and incidents.	Prepare	1	It is important to document the incidents that have already occurred and how they were mitigated to be prepared for future instances (U.S. Department of Energy, 2022).
2.2.1 The organization has an institutionalized malware prevention program.	Protect	1	The organization should have industry standard malware prevention installed on all the organizational systems to protect against threats (U.S. Department of Energy, 2022).
2.4.2 Constituents are provided with security education, training, and awareness (ETA).	Protect	1	Staff training is an important aspect as untrained staff are prone to attacks as they might make human errors and accidently leak company data which in this case is medical records and would have severe consequences (Center for Internet Security, n.d.).
3.1.1 Security monitoring is continuously performed on all constituent networks and systems.	Detect	1	Monitoring the systems and networks is crucial for seamless business operation as it can lead to discovery of vulnerabilities in the system (U.S. Department of Energy, 2022).
4.1.2 Incidents are reported to appropriate	Respond	1	Incident reporting to respective stakeholders such as CISO and the executive board as it helps them in

management in accordance with organizational guidelines.			understanding the importance of the incident management development (Australian Government, n.d.).
4.1.3 Incidents are reported to and coordinated with the appropriate external organizations or groups in accordance with organizational guidelines	Respond	1	As per the Notifiable Data Breaches (NDB) scheme and Office of the Australian Information Commissioner (OAIC) the affected parties and the government has to be notified about the breaches (Australian Government, n.d.).
4.3.2 Incidents are resolved.	Respond	1	Resolving the incident, analysing the cause and documenting the procedure is an important aspect (U.S. Department of Energy, 2022).
5.2.4 A quality assurance (QA) program exists to ensure the quality of provided products and services.	Sustain	2	The QA plays a vital role in the robustness of the incident management mechanism, some aspects is covers include (puredome, n.d.): • Spotting any prevalent weakness • Continuous improvement.

CURRENT MATURITY MODEL

Upon investigation it is evident the current maturity model is at a basic level MIL1 which states that Initial practices are performed but may be ad hoc as it lacks any formal process but are in the stage of development (U.S. Department of Energy, 2022).

Justification for the level 1 are as follows:

Ad Hoc Incident Response: No official incident management function or CSIRT, leading to inconsistent and uncoordinated responses.

Inadequate Policy Framework: Lack of a comprehensive incident management plan, business continuity policy, or data protection strategies.

Limited Security Awareness: Insufficient staff training, leaving employees vulnerable to phishing and other attacks.

No Continuous Monitoring: Absence of continuous security monitoring and central repository for incident documentation, hindering threat detection and learning from past incidents.

No External Coordination: Lack of established protocols for reporting incidents to external organizations, risking non-compliance with regulations.

PROPOSED ROAD MAP

Designate a CSIRT: Within 30 days, appoint a dedicated team to handle cybersecurity incidents, ensuring a clear point of contact for incident management (Florida Department of Transportation, 2020).

Develop an Incident Management Plan: Within 60 days, create a comprehensive plan covering identification, communication, and recovery, tailored to the hospital's needs (U.S. Department of Energy, 2022).

Implement Staff Training: Roll out mandatory cybersecurity training for all staff within 90 days to address phishing and other threats (McCrohan, Engel, & Harvey, 2010).

Establish Continuous Monitoring: Deploy monitoring tools across all systems within 120 days to detect and respond to threats in real-time (U.S. Department of Energy, 2022).

Create a Central Repository: Within 150 days, develop a centralized database for logging and tracking security incidents to facilitate future learning and improvements (U.S. Department of Energy, 2022).

Coordinate with External Bodies: Within 180 days, establish protocols for reporting incidents to regulatory bodies and external partners, ensuring compliance and transparency (U.S. Department of Energy, 2022, Florida Department of Transportation, 2020).

CONCLUSION

The proposed roadmap addresses Zenith Hospital's cybersecurity weaknesses, enhancing incident management, staff training, monitoring, and compliance, ultimately elevating the hospital's cybersecurity maturity and resilience

REFERENCES

Nduhiu, J. (2023, February 27). *What are CSIRTs or CERTs?* Splunk a CISCO Company. https://www.splunk.com/en_us/blog/learn/csirt-computer-security-incident-response-team.html#

Atlassian (n.d.). *What is incident management?* https://www.atlassian.com/incident-management#the-importance-of-incident-management

U.S. Department of Energy. (2022). *C2M2 Version 2.1 June 2022* [PDF]. Cybersecurity Capability Maturity Model (C2M2). https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

Center for Internet Security (n.d.). *Why Employee Cybersecurity Awareness Training Is Important*. https://www.cisecurity.org/insights/blog/why-employee-cybersecurity-awareness-training-is-important

Australian Government (n.d.). About the Notifiable Data Breaches scheme. Australian Government Office of the Australian Information Commissioner. https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme

Tuffley, D. (n.d.). 4.5 Incident Management Capabilities. LMS Griffith University. https://lms.griffith.edu.au/courses/23641/pages/4-dot-5-incident-management-capabilities?module_item_id=577650

puredome (n.d.). *The Crucial Role of Cyber Security Quality Assurance*. https://www.puredome.com/blog/cyber-security-quality-assurance#

Florida Department of Transportation. (2020). *Transportation technology manual: Computer security incident response team (CSIRT) (Topic No. 325-000-002, Effective 07-01-2020).* https://www.fdot.gov/docs/default-source/it/oitmanual/Chapter1ComputerSecurityIncidentResponse.pdf

McCrohan, K. F., Engel, K., & Harvey, J. W. (2010). Influence of awareness and training on cyber security. Journal of internet Commerce, 9(1), 23-41.

MODULE 5: ETHICAL AI CASE STUDY ANALYSIS

TechnoCore: Ethics V/S Cost

INTRODUCTION

The analysis is conducted on dilemma faced by TechnoCore which is an AI company and have developed a ML model to optimize the screening process however the data used for the training of ML model was biased towards certain communities and have now affected the whole process by marginalizing those communities as their resumes are not going through and are being removed in the very first stage. On one hand the model itself is saving money for the organization but at the same time it is costing deserving individuals their spot.

KEY ETHICAL ISSUES IDENTIFIED

Biasness and Discrimination: the ML model exhibits biasness towards minorities and is more inclined towards white male individuals giving them an unfair advantage. This issue contributes to hinder people's ability to actively participate in the economy and society as many competent individuals might not get their deserved chance (IBM, 2023; Larkin, 2022; McKinsey & Company, 2019)

Fairness and Justice: The candidates are unfairly judged on the basis of their attributes that include gender, ethnical and religious background, previous non-conventional roles. This is not only a problem on an individual level but on an organizational level as well, because the organization is now prone to legal implications for discrimination(Australian Government, n.d.).

Transparency and Accountability: Another important problem identified is the lack of transparency and accountability of TechnoCore using the ML model, the first instance of biasness identified should have been enough for the organization to deter from the practice and work on fixing it however they failed to investigate on a deeper level why the data collected and used for training was biased to begin with (Del Pero, Wyckoff, & Vourc'h, 2022; Wren, 2024)

PRIORITIZATION OF ISSUES BASED ON ETHICAL PRINCIPLES:

The table below highlights the issue and also has the relevant ethical principles to justify the issue.

Issue	Ethical Framework	Justification
Biasness and Discrimination	ACS, The Universal Moral Code	The two selected ethical code of conducts focus on the public interest to ensure that the general public inclusive of all irrespective of cast, creed, colour, gender and religion are kept at the centre and given them their due

		share. The other aspect is to not harm anyone, not to cheat out anyone from what they deserve (ACS, 2023; University of Oxford, n.d.).
Fairness and Justice	ACS, Kantianism	Combined the two ethical codes focus on honesty and treating people fairly which stems from the concept of asking oneself if they are exploiting someone to attain their desired goals, which in the case of TechnoCore is that they are considering cost efficient method over fair process (ACS, 2023; Vleeschauwer, 2023).
Transparency	ACS	Focus is on professionalism in-order to increase the integrity of your organizational practices by being transparent with your peers and the community (ACS, 2023).

RECOMMENDED SOLUTION AND RATIONALE FOR ETHICAL JUSTIFICATION

- Retrain the Model with Diverse Data: TechnoCore should gather a more representative dataset that includes resumes from diverse backgrounds, ensuring the model is trained to fairly evaluate all candidates (IBM, 2023).
- Implement Bias Detection Tools: Introduce tools that regularly assess and correct biases within the AI model, ensuring continuous improvement in fairness and reducing the risk of discrimination (Wren, 2024).
- Increase Transparency: Make the AI screening process transparent by providing candidates with explanations for decisions, helping to build trust and accountability within the hiring process (Del Pero, Wyckoff, & Vourc'h, 2022).
- Conduct Regular Audits: Establish regular audits of the AI system to ensure ongoing compliance with ethical standards and legal requirements, preventing biased outcomes from recurring (Australian Government, n.d.).
- Develop an Ethical AI Governance Policy: Create and enforce a comprehensive policy that outlines the ethical use of AI, focusing on fairness, transparency, and accountability in decision-making processes (Larkin, 2022).

CONCLUSION

TechnoCore must prioritize fairness and transparency by retraining their AI model, implementing bias detection, and enforcing ethical policies, ensuring a more equitable and legally compliant hiring process.

REFERENCES

IBM (2023, October 16). Shedding light on AI bias with real world examples. https://www.ibm.com/think/topics/shedding-light-on-ai-bias-with-real-world-examples

Larkin, Z. (2022, November 16). *AI Bias - What Is It and How to Avoid It?* https://levity.ai/blog/ai-bias-how-to-avoid

McKinsey & Company (2019, June 6). *Tackling bias in artificial intelligence (and in humans)*. https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans

Australian Government (n.d.). *Workplace discrimination*. Fair Work Ombudsman. https://www.fairwork.gov.au/tools-and-resources/fact-sheets/rights-and-obligations/workplace-discrimination

Del Pero, A. S., Wyckoff, P., & Vourc'h, A. (2022). Using Artificial Intelligence in the workplace: What are the main ethical risks?

Wren, H. (2024, January 18). *What is AI transparency? A comprehensive guide*. https://www.zendesk.com/au/blog/ai-transparency/

ACS (2023). *Professional Ethics, Conduct and Complaints*. https://www.acs.org.au/memberships/professional-ethics-conduct-and-complaints.html

University of Oxford (n.d.). *Seven moral rules found all around the world*. https://www.ox.ac.uk/news/2019-02-11-seven-moral-rules-found-all-around-world

Vleeschauwer, H. Jean de (2023, March 2). Kantianism. Encyclopedia Britannica. https://www.britannica.com/topic/Kantianism