dd dd

ISYS1002-Assignment 3 (1).docx

My Files

My Files

University

Document Details

Submission ID

trn:oid:::3618:108671579

Submission Date

Aug 18, 2025, 12:16 AM GMT+5:30

Download Date

Aug 18, 2025, 12:17 AM GMT+5:30

File Name

ISYS1002-Assignment 3 (1).docx

File Size

80.1 KB

16 Pages

2,634 Words

15,142 Characters

16% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography

Match Groups

17 Not Cited or Quoted 13%
Matches with neither in-text citation nor quotation marks

5 Missing Quotations 4%
Matches that are still very similar to source material

0 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

4% Internet sources
0% Publications
16% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any inconsistencies that would set it apart from a normal submission. If we notice something strange, we flag it for you to review.

A Flag is not necessarily an indicator of a problem. However, we'd recommend you focus your attention there for further review.

Match Groups

- **17** Not Cited or Quoted 13%
  Matches with neither in-text citation nor quotation marks
- **5** Missing Quotations 4%
  Matches that are still very similar to source material
- **0** Missing Citation 0%
  Matches that have quotation marks, but no in-text citation
- **0** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

- 4% Internet sources
- 0% Publications
- 16% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Submitted works	Southern Cross University on 2025-08-04 — 13%
2	Internet	fastercapital.com — 1%
3	Submitted works	Southern Cross University on 2025-08-04 — <1%
4	Submitted works	Southern Cross University on 2025-08-05 — <1%
5	Submitted works	Southern Cross University on 2023-07-23 — <1%
6	Submitted works	Southern Cross University on 2025-08-17 — <1%
7	Submitted works	Southern Cross University on 2025-08-17 — <1%
8	Internet	real.mtak.hu — <1%
9	Internet	www.utupub.fi — <1%

Southern Cross University

ISYS1002-ASSIGNMENT-3

Declaration:

I have read and understood the Rules Relating to Awards (Rule 3 Section 18 – Academic Misconduct Including Plagiarism) as contained in the SCU Policy Library.
I understand the penalties that apply for plagiarism and agree to be bound by these rules. The work I am submitting electronically is entirely my own work.

Student Full Name:Ashraful Haque
Student email address: a.haque.11@student.scu.edu.au

This page left blank intentionally..

TABLE OF CONTENTS

Executive Summary

In this report, the BYOD (Bring your own device) and work-at-home policies have been evaluated with regards to the critical assets of the organization that comprise Customer PII & Account Data (CRM), Billing and Payment Systems (BSS), Identity and Access Management (IDAM), Mobile Core Network (HLR/HSS, EPC / 5GC), and Customer Web / Client Portals and APIs. Although, these policies provide flexibility and efficiency to the organization, they have a big toll on cybersecurity of the organization, particularly those which are highly sensitive and necessary to the organization.The evaluation reveals the main threats of the insider misuse, phishing attacks, ransomware, and account takeover that are enhanced by the use of personal devices and work in the enterprise remotely. All of the highly valuable assets have vulnerabilities associated with poor authentication, device management, insecure APIs, and untimely patching, which may cause a massive financial and reputational loss. There is a qualitative risk assessment process that is utilized to classify the risks in terms of their likelihood and impact. The Customer PII and Billing Systems are observed to be in a critical risk with other assets such as IDAM and Mobile Core Network also being in the high-risk category. In order to combat such risks, the prevention suggestions would involve enforcing Multi-Factor Authentication (MFA), enhancing device management, DDoS protection and frequent review of security. Such actions are vital in preventing losses to the organization as well as continuity of its business activities.To sum up, as valuable as BYOD and working-at-home policies are to the modern workplace, cybersecurity is the way to ensure that important information and essential systems are not affected by the evolving threats.

1. Introduction

Over the last few years, the number of companies using Bring Your Own Device (BYOD) and work-at-home policies as their digitalization trends has been growing. Such policies are flexible, less expensive, and more productive of the employees as they permit them to use personal devices and work remotely. Nevertheless, although such policies have a number of advantages, they also have an equal number of cybersecurity threats, which one has to handle with caution. The security of personal gadgets used as work machines can vary with that of gadgets serviced by corporations, thus leaving the organization at the risk of cyber risk through exposure to vital organizational assets. There is also a danger of data tampering, unauthorized read-ins, and cyber-attacks when working remotely because workers could enter the corporate systems using less-secure home devices and unsecured open networks.

In the case of organizations such as Telstra (source as used in Assignment 2), protection of critical assets, which include data such as Customer PII & Account Data (CRM), Billing & Payment Systems (BSS), Identity & Access Management (IDAM), Mobile Core Network (HLR/HSS, EPC/5GC), and Customer Web/App Portals & APIs becomes even more difficult when the BYOD and work-at-home policies are active. The policies have the potential to compromise the security regimes in terms of access controls, data encryption and network security among others posing a greater risk of cyber threats and vulnerabilities that must be dealt with.

The purpose of this report is to evaluate the cybersecurity risk of BYOD, work-at-home policies and make suggestions on the practices that should be carried out to reduce the risk liability bearing in mind the identified critical assets. This will be measured according to the CIA Triad, Confidentiality, Integrity, Availability, which gives a framework that will be used to measure the effect of such policies on organizational security.

2. Critical Assets and Their Security Needs (CIA Triad)

The Customer PII & Account Data (CRM), Billing and Payment Systems (BSS), Identity and Access Management, Mobile Core Network (HLR/HSS, EPC/5GC), and Customer Web/App Portals and APIs are the most important assets of the organization. The business needs to afford protection to these assets which are vital to the smooth running of the business in these three sections of the CIA Triad, namely Confidentiality, Integrity, and Availability.

Asset	Confidentiality	Integrity	Availability
Customer PII & Account Data (CRM)	Protecting personal and financial information	Ensuring accuracy and consistency of customer data	Ensuring timely access for customer service and transactions
Billing & Payment Systems (BSS)	Safeguarding billing and payment information	Preventing unauthorized alterations to billing data	Ensuring system uptime during billing cycles
Identity & Access Management (IDAM)	Securing authentication credentials and access controls	Ensuring proper user roles and permissions	Maintaining continuous authentication services
Mobile Core Network (HLR/HSS, EPC/5GC)	Protecting user communication data	Ensuring accurate user profiles and service records	Ensuring uninterrupted mobile network services
Customer Web/App Portals & APIs	Securing user interactions and data	Ensuring data integrity during transactions	Providing consistent access to online services

The security requirements of these assets in terms of the CIA Triad designate the type of cybersecurity that should be implemented in order to secure them accordingly. The specific security measures need to be applied to secure every asset against external and internal threats.

3. Identified Threats and Vulnerabilities

The security specifications of such assets related to the CIA Triad determine what kind of cybersecurity would apply in securing such assets effectively. The particular security guard must be put in place to protect all the assets against external and internal threats.

1. Account Data (CRM) Customer PII

Threats:

- Misuse by Insiders: Insiders, who may have fingertip access and access to sensitive customer information on their personal phones and devices, are likely to steal the information, or misuse it to the potential harm of the information holder. Thec devices personalized are not always endowed with the same security guidelines that the systems under the management of the corporations have, and this is a risk of the data breach.
- Phishing Attacks: Phishing attacks are usually employed in order to steal log in details or delicate information provided by remote employees. Attackers can attack through phishing emails or fake websites that can attack employees and find out their account details to destroy the access to the CRM systems (Hashemi-Pour & Chai, 2023).

Vulnerabilities:

- Insufficient Device Management: Personal devices brought into the working environment might not be installed with security facilities like encryption, firewalls, and anti-virus software which can allow them to contract malware infections and be accessed by third parties.
- Weak Authentication: Unauthorized access to CRM systems can be done by unauthorized users since in case of not using Multi-Factor Authentication (MFA) on personal devices, the customer data will be at risk.

2. Billing & Payment Systems BSS

Threats:

- Ransomware Attacks: Remote employees who connect to the billing system of the organization via personal devices increase the chance of malware spread, including ransomware. Hackers have the ability to put important billing information on lockdown, ultimately forcing transactions at a ransom (Remote, Controlled, n.d.).
- Fraudulent Billing: Insecure device configuration can permit attackers to modify billing data, alter the amount of a transaction or instead of making a payment.

Vulnerabilities:

- Personal Devices: The personal devices can be used to bypass security checks on the billing systems by using weak input validation. Malicious programs may be crossed into these weaknesses to introduce malevolent information or even modify financial deals.
- Untested Backup Procedures: Untested backup procedures since, with remote work, it is entirely possible that the backup systems do not undergo regular testing, leaving areas where recovery procedures are not followed after any incidents or ransomware attacks.

3. ID Range, Identity & Access Management (IDAM)

Threats:

- MFA Bypass with Phishing: Phishing kits have also become common tools that attackers use to fool employees into entering their credentials and bypassing MFA defenses, which results in the unauthorized access of sensitive systems (Hashemi-Pour & Chai, 2023).
- Session Hijacking: Working remotely can lead those workers to open their sessions to attackers often without their knowledge particularly when their personal devices are infected. This may cause hijacking of a session whereby enemies assume the commission of a legitimate user by stealing a legitimate session token.

Vulnerabilities:

- Excessive Permissions: Personal device used at work would leave room over time to acquire excessive permissions. Role management can go wrong, and when this is not done well, the challenge of privilege escalation is possible to enable the access to sensitive systems by the unauthorized person.
- Insecure Remote Access: Personal devices through which remote work is done might not provide adequate VPN encryption or access point encryption and increases the susceptibility of the access points increasing chances of unauthorized logins.

4. Mobile Core Network (HLR/HSS,EPCHL5GC)

Threats:

- DDoS Attacks: The home workers who may connect to the mobile core networks via unsecured networks can easily expose the network to Distributed Denial of Service (DDoS) attacks which can affect critical control plane services resulting in the disruption of services (Cybersecurity Framework | NIST, 2025).
- Signaling Manipulation: Hackers might attack SS7, Diameter or 5G signaling protocol communicated on the mobile core network. Such attacks may eavesdrop or redirect calls and mobile data, which poses a huge inconvenience and interruption of data.

Vulnerabilities:

- Patch Delays: Personal devices can be lagging behind on updates of their devices leaving known weaknesses open to attack. Late coverage of patching of components of the core network of mobile networks may create dangerous theological holes and this may be exploited by cybercriminals.
- Configuration Drift: Workers stationed at distant places might set their mobile devices in a way that brings security loopholes into the network set up that cannot be easily realized unless there is proper monitoring.

5. APIs & Customer Web/App Portals

Threats:

- Account Takeover (ATO): Personal devices that are available to remote workers can be compromised, which will result in Account Takeover (ATO) attacks as attackers can log to customer accounts and carry out malicious activities using stolen credentials (IBM Industry Solutions, n.d.).
- Unsecure APIs: It is possible APIs utilized by the customer-facing systems are not being appropriately secured on personal devices, opening up the potential of information getting leaked or other individuals having unauthorized access to critical user data.

Vulnerabilities:

- Insufficient object-level authority: APIs without object-level authority are exposed to Insecure Direct Object References (IDOR), where attackers can control or even access data that they do not own, and they are not supposed to, even in multi-user contexts (Hashemi-Pour & Chai, 2023).
- Security Concerns with Legacy Devices: Older web applications that are less secure, e.g., do not support more modern security mechanisms, like anti-CSRF tokens or secure cookies, can also become exposed to an increased risk of attacks, e.g., Cross-Site Request Forgery (CSRF).

4. Risk Assessment Process

Risk Assessment Process uses a qualitative analysis to analyze the risks that are potential threats to critical assets of the organization through a qualitative process in light of the BYOD and work-at-home policies of the organization. Under this approach, the probability (the likelihood of occurrence) and the impact (consequences of occurrence) of each of the identified threats is evaluated leading to a risk rating. Using such two factors, the risk matrix employed in this assessment classifies every risk under low, medium, and high levels.

This process starts with an identification of threats and vulnerabilities, which are considered further in relation to their probability and the consequences they may cause to the organization. This assists to determine the most important potential dangers that require immediate attention and counteraction.

Each of the five critical assets will be rated based on its potential likelihood of a threat occurring and its potential impact and these include Customer PII & Account Data (CRM), Billing & Payment Systems (BSS), Identity & Access Management (IDAM), Mobile Core Network (HLR/HSS, EPC/5GC) and Customer Web/App Portals & APIs. Its probability is classified as Low, Medium, or High basing on the rate at which the threat has affected similar organization or environment. The effects are rated in an identical manner relying on the harm or loss that may come about because of the threat.

The following is the Risk Matrix applicable in this assessment:

Likelihood / Impact	Low	Medium	High
Low	Low Risk	Medium Risk	High Risk
Medium	Medium Risk	High Risk	Critical Risk
High	High Risk	Critical Risk	Critical Risk

The risks associated with each critical asset are categorized and rated as follows:

- **Customer PII & Account Data (CRM):** There are a high probability of insider misuse and phishing attacks because of remote working habits. The impact is also extremely high since the unauthorized access to the customer data can result in the noticeable reputational and financial loss. This gives a vital risk classification.
- **Billing & Payment Systems (BSS)**: **Ransomware attacks** and **fraudulent billing** also pose a high risk due to remote access and unsecured personal devices. The **impact** is high since billing disruptions can cause revenue loss and operational downtime. The rating for this asset is **high risk**.
- **Identity & Access Management (IDAM)**: The threat of **MFA bypass** and **session hijacking** has a **medium likelihood**, but the **impact** is high because compromised credentials can lead to widespread system access. The **risk** rating for IDAM is **high risk**.

- **Mobile Core Network (HLR/HSS, EPC/5GC)**: The threat of **DDoS attacks** and **signaling manipulation** has a **medium likelihood** due to the scale and complexity of such attacks. However, the **impact** is critical as it can cause nationwide service disruptions. This results in a **high risk** rating.

- **Customer Web/App Portals & APIs**: **Account Takeover (ATO)** and **API abuse** have a **high likelihood** due to frequent exposure to cyberattacks. The **impact** is medium, as compromised accounts can damage customer trust and affect service quality. The rating for this asset is **high risk**.

Risk Matrix for Each Asset

Asset	Threat	Likelihood	Impact	Risk Rating
Customer PII & Account Data (CRM)	Insider misuse, Phishing attacks	High	High	Critical Risk
Billing & Payment Systems (BSS)	Ransomware, Fraudulent billing	High	High	High Risk
Identity & Access Management (IDAM)	MFA bypass, Session hijacking	Medium	High	High Risk
Mobile Core Network (HLR/HSS, EPC/5GC)	DDoS, Signaling manipulation	Medium	Critical	High Risk
Customer Web/App Portals & APIs	Account Takeover (ATO), API abuse	High	Medium	High Risk

5. Conclusion

The access point of this report evaluated the cybersecurity hazard to the five critical assets of the organization, which are Customer PII & Account Data (CRM), Billing & Payment Systems (BSS), Identity & Access Management (IDAM), Mobile Core Network (HLR/HSS, EPC/5GC), and Customer Web/App Portals & APIs, through BYOD and working-at-home policies. The qualitative risk analysis showed that risks to such assets are quite high especially the insider misuse, phishing, ransomware, and session hijacking. The practice of using personal devices and remote work creates many of these risks.

Customer PII and Billing Systems pose the greatest danger since there are high probabilities of their compromise and resultant serious financial and reputational losses. Other properties such as IDAM and Mobile Core Network remain to be the very risky assets only that the chances of attack are a bit lower.

In providing mitigation of this risk, the report advises the implementation of effective security practices, including Multi-Factor Authentication (MFA), sophisticated threat detection, device security control and patching. It shall equally be important to enhance security around the network and use of access controls so as to guarantee this kind of asset against changing cyber threats.

References (APA style)

Cybersecurity Framework | NIST. (2025, August 5). National Institute of Standards and Technology. https://www.nist.gov/cyberframework

Hashemi-Pour, C., & Chai, W. (2023, December 21). What is the CIA triad (confidentiality, integrity and availability)? WhatIs. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

IBM Industry Solutions. (n.d.). https://www.ibm.com/industries

Remote, controlled. (n.d.). Deloitte. https://www.deloitte.com/global/en/services/tax/research/global-tax-remote-work-survey.html

Report Highlight for market trends: All-in-One desktop opportunity arises. (n.d.). Gartner. https://www.gartner.com/en/documents/2461015

Acknowledgement Statement

"I acknowledge that I have not used GenAI to complete this assessment."