University of the Western Cape

Faculty of Economic and Management Sciences

Department of Political Studies

Name and Surname	**Student Number**
Nieyaaz Abrahams	4495086
Ethan Rhode	4496463
Tazkia Ismail	4495304
Azaad Hendricks	4497151
Vuyo Mangaliso	4494374

Module Code: IFS 132

Lecturer:

Tutor: Chulumanco Manzini

Tutorial Group number: 2

Assignment: Group Assignment – Cyber Security

Submission Date: 31st August 2024

Plagiarism Declaration

1. This summary/ exercise is my own work, and not plagiarized in any way. Plagiarism is to use another's work and pretend it is one's own.
2. I know plagiarism is wrong. Plagiarism is to use another person's work and present it as one's own.
3. Each significant contribution to, and direct quotation in this assignment that I have taken from the works of other authors has been acknowledged and referenced. I have not copied texts of more than 10 words without a reference.
4. I have not allowed, and will not allow anyone to copy my work with the intention of passing it off as his or her work.
5. I am aware of the fact that plagiarism could lead to the canceling of my marks and, in serious cases, to expulsion from the university.

Signed: *N. Abrahams ,EL.Rhode , T .Ismail , V. Mangaliso, A.Hendricks*

Date: August 2024

Table of contents

Introduction

Given the recent ransomware attack on the National Health Laboratory Services (NHLS), MASE Inc. has to evaluate any potential cybersecurity risks that could harm both its employees and other businesses in the sector. The purpose of this report is to give the Board of Directors a thorough study by outlining the cybersecurity dangers that exist today, the techniques used to recognize and evaluate these risks, and the conclusions drawn from our research. The paper will also examine the consequences of these discoveries, namely the difficulties they provide for MASE Inc. and related entities. To keep MASE Inc. strong in the face of a constantly evolving threat landscape, we will lastly suggest practical ways to reduce these cybersecurity risks.

The importance of addressing cybersecurity threats:

Organizations like NHLS are depending more and more on digital systems to run their business in today's linked environment. Although there are many advantages to this digital transformation, these organizations are also more vulnerable to ransomware, phishing, and advanced persistent threats (APTs), among other cybersecurity risks. A sobering reminder of the catastrophic effects that cyberattacks can have on vital infrastructure is the recent ransomware attack on NHLS. These attacks not only cause operational disruptions, but they may also result in large monetary losses, legal ramifications, and harm to one's reputation .

It follows that addressing cybersecurity threats is crucial. The stakes are even higher for organizations like NHLS that deal with sensitive health data. If a hack is successful, personal health information may be disclosed without authorisation, which might have catastrophic repercussions for those who are impacted. Moreover, any disruption to the availability and integrity of health data could have fatal effects for the efficient operation of healthcare services .

Organizations need to take a proactive stance when it comes to cybersecurity in order to reduce these risks. This entails putting in place strong security measures, evaluating vulnerabilities on a regular basis, and informing staff members of the significance of cybersecurity. By doing this, businesses can lessen the chance that a cyberattack will be successful and lessen the effects of any breaches that happen. All organizations should prioritize cybersecurity and make sure they are sufficiently secured against the constantly changing threat landscape in light of the NHLS incident.

What are Cybersecurity threats

A major ransomware attack recently affected the National Health Laboratory Services (NHLS) and had far-reaching effects on the organization's operations and data integrity. Critical health data was encrypted as a result of the assault, seriously impairing laboratory services throughout South Africa. NHLS serves as the foundation for public health diagnostics, enabling millions of patients to receive medical testing that informs their treatment choices. Patient care may have been jeopardized due to the disturbance in diagnosis and treatment brought on by the data encryption. NHLS brought attention to the vulnerability of crucial public health infrastructure to cyber threats and the pressing need for strong cybersecurity measures after they were forced to make the difficult choice of either paying a ransom to recover access to their data or trying to restore their systems independently.

Cybersecurity threats

Organizations face serious difficulties as a result of cybersecurity threats, especially in industries like healthcare where service continuity and data integrity are vital. Ransomware is one of the worst threats; it is a kind of malicious software that encrypts files and demands a fee to unlock them. The impact of ransomware attacks, which have resulted in interruptions to critical services, potential data loss, and substantial financial expenditures, is exemplified by the recent attack on the National Health Laboratory Services (NHLS) in South Africa . Similar to this, phishing assaults can lead to credential theft and illegal access to networks since they entail deceptive attempts to collect sensitive information by impersonating reliable organizations .

Other serious risks include advanced persistent threats (APTs), which are deliberate, long-lasting attacks by skilled adversaries hoping to stealthily exfiltrate data over an extended period of time, and insider threats, which occur when workers or contractors, either intentionally or unintentionally, cause data breaches or sabotage . Further increasing security dangers are zero-day exploits, which target unpatched vulnerabilities and potentially affect systems before updates are released. When taken as a whole, these dangers highlight the necessity of strong cybersecurity defenses against the always changing array of assaults.

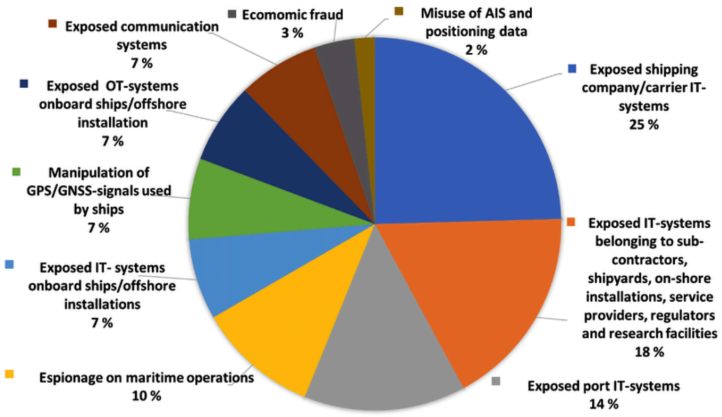
Risk Reduction Strategies

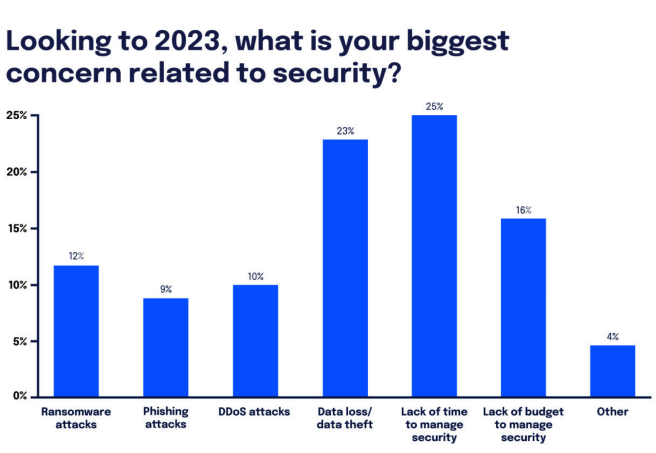
Organizations need to put strong backup systems in place that guarantee regular backups of important data and offline storage of that data in order to reduce cybersecurity threats. Because it enables data recovery without requiring payment of a ransom, this method guards against data loss during occurrences such as ransomware attacks . Since phishing is still a popular attack vector, improving email security is also essential. By using sophisticated spam filters and email verification procedures, organizations can lower the likelihood that phishing efforts will be successful.

Employees must receive regular security training in addition to technical defenses. The probability of human error resulting in a security breach can be considerably decreased by training employees on how to identify and handle threats, such as phishing emails and social engineering attempts. Role-based access and multi-factor authentication (MFA) are two ways to strengthen access restrictions and add an extra layer of security to make sure that only authorized users can access critical data and systems.

It is crucial to conduct frequent vulnerability assessments and timely patch management in order to detect and resolve any potential security flaws before they are taken advantage of. Furthermore, creating a thorough incident response strategy guarantees that businesses are ready to react quickly and efficiently to security breaches, reducing harm and promoting a quicker recovery. When combined, these tactics form a multi-tiered defense that dramatically lowers the danger of cyberattacks

A Graph representing the main threats to cybersecurity:





Methods of inquiry of cybersecurity:

In the field of cybersecurity, there are several methods used to address various aspects. The common methods are usually:

Risk Assessment:

This method is used to identify and prioritize risks to an organization's information assets. There are two main approaches:**Qualitative Risk Assessmen**t: This evaluates risks based on subjective criteria.**Quantitative Risk Assessment**: This uses numerical values to assess the likelihood and impact of risks.

Threat Intelligence:

The purpose of this method is to gather and analyze information about potential threats and adversaries. There are three main methods:**Open-Source Intelligence (OSINT):** This collects information from publicly available sources.**Human Intelligence (HUMINT)**: This gathers information through interpersonal interactions.**Technical Intelligence (TECHINT):** This method analyzes technical data, such as malware samples.

Vulnerability Assessment:

This method is used to identify and evaluate weaknesses in systems. There are two main methods:**Automated Scanning:** This uses tools to scan for known vulnerabilities.**Manual Testing:** This involves manual inspection and testing for vulnerabilities

Penetration Testing (Ethical Hacking):

The purpose of this method is to simulate attacks and identify vulnerabilities that could be exploited. There are three main approaches:**Black-Box Testing:** Testers have no prior knowledge of the system.**White-Box Testing:** Testers have a full understanding of the system.**Gray-Box Testing:** Testers have a partial understanding of the system.

Forensic Analysis:

This method is used to investigate and analyze cyber incidents to understand their nature and impact. There are **two** main methods:**Digital Forensics**: This analyzes digital evidence from computers, mobile devices, and Networks.**Network Forensics**: This focuses on network traffic and logs to trace cyber incidents.

Appendix A: Risk Assessment Procedures

Objective: The aim is to identify and evaluate potential risks to MASE Inc.'s information Assets.**Risk Identification:** This outlines the process for identifying possible threats and Vulnerabilities.**Risk Analysis:** Techniques for assessing the likelihood and impact of identified risks(e.g., qualitative, quantitative).**Risk Evaluation**: Criteria for prioritizing risks based on their potential impact on the Organization.**Mitigation Strategies:** Approaches for mitigating identified risks.

Appendix B: Threat Intelligence Gathering

Objective: To collect and analyze information about potential threats to MASE Inc.
Data Sources: A list of internal and external sources for threat intelligence (e.g., OSINT, commercial threat feeds).**Analysis Techniques:** Methods for analyzing and interpreting threat data (e.g., pattern recognition, trend analysis).
Integration: The process for integrating threat intelligence into the security posture of MASE Inc.

Appendix C: Vulnerability Assessment

Objective: To identify and assess vulnerabilities within MASE Inc.'s systems and Networks.**Scanning Tools:** A list and description of tools used for automated vulnerability scanning.**Manual Testing Procedures:** Guidelines for performing manual vulnerability assessments.**Reporting and Remediation:** The process for documenting findings and implementing remediation measures.

Appendix D: Penetration Testing Protocols

Objective: To simulate attacks to discover and address potential security weaknesses.
Methods:**Testing Scope:** Definition of the scope and objectives of penetration tests.
Testing Types: Description of different types of penetration tests (black-box, white-box, gray-box).**Execution:** Procedures for conducting penetration tests, including pre-test preparation and post-test reporting.

Risk Assessment Solutions:

Introduce a risk management framework.**Tools:** Employ risk management tools such as RiskWatch or Qualys for automated risk Assessments**.Frameworks:** Adopt structured risk management frameworks like NIST Risk Management Framework (RMF) or ISO/IEC 27005.**Process:** Develop a formal risk assessment process covering identification, analysis,evaluation, and treatment of risks. Update risk assessments regularly to reflect environmental changes.

Threat Intelligence Solutions:

Utilize advanced threat intelligence platforms and integration methods.Tools: Deploy threat intelligence platforms like Recorded Future, ThreatConnect,or Anomaly.Integration: Integrate threat intelligence feeds with your Security Information and Event Management (SIEM) system to enhance detection capabilities.Process: Establish a threat intelligence program for gathering, analyzing, and disseminating relevant threat information.

Vulnerability Assessment Solutions

Implement a combination of automated and manual vulnerability management Tools.**Tools:** Automate scanning tools like Nessus, Qualys, or OpenVAS to identify Vulnerabilities.**Manual Testing:** Conduct periodic manual assessments using tools like Burp Suite or Nmap for in-depth analysis.**Process:** Create a vulnerability management process involving regular scans,prioritization of vulnerabilities, and remediation efforts.

Penetration Testing Solutions:Solution:

Conduct regular and comprehensive penetration testing. **Tools:** Utilize penetration testing tools such as Metasploit, Kali Linux, or Core Impact.**Service Providers**: Engage with professional penetration testing service providers for thorough and independent testing.Process:Develop a penetration testing schedule and ensure that results are documented and utilized to improve security posture.

Forensic Analysis Solutions:

Implement a forensic investigation process and tools.Tools:Use digital forensic tools like EnCase, FTK Imager, or Sleuth Kit for evidence collection and analysis.Process: Establish a forensic response plan covering evidence preservation, analysis, and reporting. Additionally, ensure that your team is well-trained in forensic methods and legal considerations

Findings of cyber security threats:

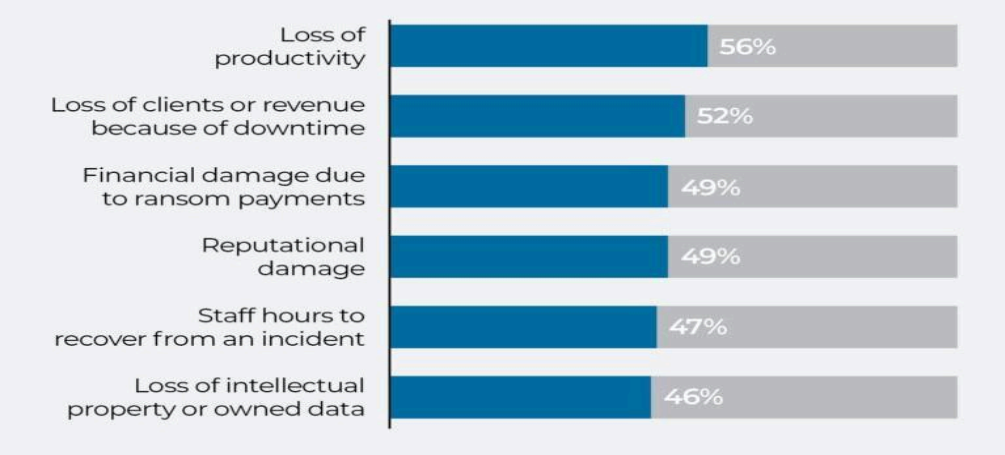
Cyber security has a major impact on companies and it is important for companies to prevent cyber-attacks by understanding what cyber security threats are, including the impacts that cyber security threats obtain and how to avoid cyber security threats. A cyber security threat is a potential attack to a company's sensitive information stored in a cloud or file in the company's database, the theft of these files or digital information can stop an organization from moving forward, furthermore the costs of recovering from a cyber-attack is expensive and it would be cost efficient to put in measures that would avoid the cyber security threats.

One of the impacts of cyber security threats is the cost, companies are required to pay huge fines as a result of not complying with data protection regulations, furthermore hackers that breach the systems of companies have become more skilful and creative with their approaches and businesses have become more reliant on digital systems. It is said that the average cost of a cyber security threat succeeding is around R49 million (SEACOM, 2024). These costs of cyber security breaches include the compensation of the clients that were affected, the marketing of the business because the company's image might have been tweaked with, and these costs also include the revenue that was impacted negatively due to the cyber security threat (SEACOM, 2024).

There are various cyber security threats but the main ones are Malware, Phishing and Ransomware. Malware is software that steals sensitive information, financial data and passwords by accessing email attachments and websites that have been hacked and a virus takes over. Phishing is when the hacker poses to be somebody or something else so they deceive whoever is accessing the system whether it be employees or customers, and the hacker then uses deception to trick the employee or customer into feeding them confidential information, phishing is frequently used when a hacker is trying to steal information such as usernames and passwords through texts, emails and even phone calls. Ransomware is when a hacker breaches a company's files and encrypts these files, as an add on the hacker demands a ransom for the decryption key needed to access the files again. With ransomware, the hacker acts as a trusted organization and sends messages to the stakeholders that contain a link to a website that leaves the stakeholders vulnerable to being hacked, once the stakeholders are on the website then their system becomes infected and the theft of sensitive information is done, encrypting files takes place, and the virus spreading to other systems happens, as a result of ransomware the financial health and reputation of the business is impacted negatively (Kala, 2023).

It is clear that the cyber security threats cause negative impacts to organizations especially financially which leaves organizations vulnerable and forces them to improve their cyber security, these findings prove that cyber security threats cause major impacts to organizations and they should be aware of them.

A Graph Showing the Impacts of Cyber Security Threats



Consequences of cybersecurity:

1. Operational Downtime:

Material Disruption of Operations With Major Delays in: Service, Productivity & Financial Loss to MASE Inc. The increase in downtime could also have a chain reaction throughout the supply chain to clients and partners if they are affected.

2. Data Breach and Loss:

This can lead to sensitive company and customer data being leaked, or even lost such as financial fraud, IP theft, exposure of confidential information. Not only fines exist, but in the event of a data breach you may be subjected to legal issues.

3. Reputational Damage:

Failure to deliver leaves you at the mercy of your clients, stakeholders and potential loss in credibility from the public Bad press from a cybersecurity incident can erode customer confidence, slipping market share and long-term damage to the brand.

4. Financial Losses:

Can lead to monetary cost on end of ransom payment, legal compliance damages and the immediate financial hit from recovery effort. There may be further financial ramifications with the loss of business opportunities and higher insurance premiums in some regions lasting well beyond this year.

5. Regulatory Non-Compliance:

Outcome: Not meeting the different data protection laws could lead to large fines, sanctions and intensified audits from regulatory entities. This can also create additional operational disruptions when the company has to meet compliance requirements after the incident.

6. Intellectual Property Theft:

Impact: The loss of proprietary data and trade secrets that can be used against you by the competition reduces your competitive edge. This may lead to decreased innovation and weaker positioning in the market.

7. Insider Threats:

Impact: Employees are then enabled to take unsanctioned actions which may be deliberate or inadvertent resulting in data breaches and malicious intent such as sabotage IT systems with further potential security violations. This can seriously damage a Company internal but also external to secure assets.

Appendices

Appendix A:

A Case Study of the NHLS Cyber Security Incident

The timeline, methods of attack and results for the compromised incident to NHLS

Appendix B:

- Top Cybersecurity Tools And Partners
- Recommended cybersecurity tools and service providers for implementation at MASE Inc., including detailed review information of their features and benefits.

Appendix C:

- Cybersecurity Training Program Plan
- An overview of the cybersecurity training program for MASE Inc. employees, with information on modules to be undertaken in respective phases and how often they will come up as well as when they should be assessed.

Appendix D:

- Incident Response Plan Format
- Mase Incident Response Plan Template: Key Detection, Containment, Eradication and Recovery Steps for Cyber Security Incident.

Conclusion

In conclusion, in the aftermath of the recent ransomware attack on the National Health Laboratory Services (NHLS), this research has thoroughly investigated the cybersecurity risks that MASE Inc. and related organizations must deal with. The report's body included a variety of cybersecurity risks and investigation techniques, offering a thorough examination of possible attack routes such supply chain vulnerabilities, ransomware, phishing, and insider threats.

Our findings highlight how important it is to have strong cybersecurity safeguards. Significant risks were identified by the analysis in relation to these threats, emphasizing the possibility of serious operational interruptions, data breaches, financial losses, and reputational harm. These results highlight the growing complexity of cyberattacks and the need for proactive security measures, which have significant consequences for MASE Inc. and other organizations. Ignoring these cybersecurity risks could have dire consequences. If MASE Inc. ignores these risks, customer information could be exposed, business operations could be disrupted, and significant financial and reputational damage could result. These difficulties also go beyond MASE Inc. and should serve as a reminder to all businesses of the need for cybersecurity readiness.

REFERENCES:

Cyber Security Threats

Thakur, K., Qiu, M., Gai, K., & Ali, M. L. (2019). *An Investigation on Cyber Security Threats and Security Models*. IEEE Xplore. https://doi.org/10.1109/CSCloud.2015.71

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. *Arabian Journal for Science and Engineering*, *45*(1). springer. https://doi.org/10.1007/s13369-019-04319-2

Peterson, D. C., Adams, A., Sanders, S., & Sanford, B. (2018). Assessing and Addressing Threats and Risks to Cybersecurity. *Frontiers of Health Services Management*, *35*(1), 23–29. https://doi.org/10.1097/hap.0000000000000040

Öğüt, H., Raghunathan, S., & Menon, N. (2010). Cyber Security Risk Management: Public Policy Implications of Correlated Risk, Imperfect Ability to Prove Loss, and Observability of Self-Protection. *Risk Analysis*, *31*(3), 497–512. https://doi.org/10.1111/j.1539-6924.2010.01478.x

Graphs: Hakon Meland, P. (2021, January). *(PDF) A Retrospective Analysis of Maritime Cyber Security Incidents*. ResearchGate. https://www.researchgate.net/publication/354657671_A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents

Report: Cybersecurity 2023. (n.d.). Www.digitalocean.com. https://www.digitalocean.com/reports/cybersecurity-smbs-2023

Findings of cybersecurity:

5 Charts That Show It Pays to Prevent a Cyberattack Rather Than Fight One | Endpoint. (2022, June 21). Tanium. https://www.tanium.com/blog/5-charts-that-show-why-it-pays-to-prevent-a-cyberattack-rather-than-fight-one/

Financial impact of security breaches is highest in SA | SEACOM. (2024). Seacom. https://seacom.co.za/news/financial-impact-of-security-breaches-is-highest-in-sa

Kala, E. M. (2023). The Impact of Cyber Security on Business: How to Protect Your Business. Open Journal of Safety Science and Technology, 13(02), 51–65. https://doi.org/10.4236/ojsst.2023.132003

Methods of inquiry

Valle, N. (2024, August 19). Cybersecurity Tools: Types, Evaluation Methods and Implementation Tips. Invgate.com; InvGate Inc. https://blog.invgate.com/cybersecurity-Tools