**COURSEWORK SUBMISSION FORM**

|  |  |  |  |
| --- | --- | --- | --- |
| **STUDENT USE** | | **STAFF USE** | |
| Module Name | Information Security | First Marker’s  (acts as signature) |  |
| Module Code | **6COSCO16C** | Second Marker’s  (acts as signature) |  |
| Lecturer Name | Nargiza Akramova | Agreed Mark |  |
| UoW Student IDs |  | **For Registrar’s office use only (hard copy submission)** | |
| WIUT Student IDs | 00010023 |
| Deadline Date | 24.02.2022 |
| Assignment Type | Individual |
| Word Count | 2504 |

**SUBMISSION INSTRUCTIONS**

**COURSEWORKS *must* be submitted in *both* HARD COPY (to the Registrar’s Office) *and* ELECTRONIC unless instructed otherwise.**

For hardcopy submission instructions refer to: <http://intranet.wiut.uz/Shared%20Documents/Forms/AllItems.aspx> - Coursework hard copy submission instructions.doc

For online submission instructions refer to: <http://intranet.wiut.uz/Shared%20Documents/Forms/AllItems.aspx> - Coursework online submission instructions.doc

|  |
| --- |
| **MARKERS FEEDBACK (Continued on the next page)** |
|  |

**Table of Contents**

[Executive Summary 2](#_Toc117483324)

Analysis of the Cyberattack to the LAUSD……………………………………………………………………..3

* Attack Vectors and Performance [3](#_Toc117483324)
* Financial/Operational Loss…………………………………………………………………………...3
* Countermeasures……………………………………………………………………………….…….4

Security Risk Management for the LAUSD5

* Overview……………………………………………………………………………………………….5
* Proposed risk management framework…………………………………………………………….5
* Implementation………………………………………………………………………………………..6

Adoption of Information Security Framework for the LAUSD [7](#_Toc117483324)

* Three IT security frameworks comparison………………………………………………………….7
* The most suitable framrwork…………………………………………………………………………8
* Future difficulties………………………………………………………………………………………8

Conclusion [9](#_Toc117483324)

[Reference List 1](#_Toc117483324)0

**Executive Summary**

When it comes to cyber-attacks, one might think that the vector mainly concerns big organizations, such as banks, social network platforms and other large businesses. However, it should be noted that even school districts with countless students generations can become a victim of malicious attacks. Los Angeles Unified School District (LAUSD) is renowned for being the second largest school district in the United States with more than 600,000 students enrolled in the school. It consists of four public high schools that accept international students. The LAUSD operates over 1,000 schools and centers, including traditional K-12 schools, magnet schools, charter schools, adult schools, and early education centers. It employs over 60,000 people, including teachers, administrators, and support staff. The mission of the LAUSD is to provide a high-quality education to all students, regardless of their background or circumstances. To achieve this mission, the district offers a wide range of academic programs and services, including special education, English language learning, gifted and talented education, and career and technical education. The campus facilities have recently undergone some improvements and now include modernized sports complexes, outdoor communal fields and quads, as well as new learning and arts centers. Likewise, the LAUSD is famous for winning the United States Academic Decathlon championships 12 times which is the best result compared to other districts in the country. Most of the outstanding high school teachers have been awarded as Educators of the year. It is also famous for a California Gold Ribbon Award achieved by distinguished academics (Educatius, 2022).

**Analysis of the Cyberattack to the LAUSD**

One notable information security incident that occurred in the LAUSD in recent years was a data breach in 2018. The ransomware attack disrupted distance learning for thousands of students, as well as the district's payroll and email systems. The attackers demanded a ransom of $40 million in Bitcoin in exchange for restoring the district's systems, but the district refused to pay. The incident was attributed to a group of cybercriminals known as the "Maze" group, which has been responsible for similar attacks on other organizations. The FBI and other law enforcement agencies were involved in the investigation, but no arrests have been made in connection with the attack. This breach affected over 500,000 students and staff members, and led to the theft of sensitive personal information, including names, birth dates, social security numbers, and other sensitive data. The hacking organization threatened the school district by releasing stolen data on the dark web if they refused to pay ransom. However, the LAUSD immediately tuned down the negotiation without questioning the amount to be paid and stated that their financial expenses are only spent for the sake of students and education. (Sequeira, 2022).

**Attack Vector and Performance**

The attack is believed to have been successful due to a number of factors, including weak security techniques, outdated software, and a lack of employee training on cybersecurity best practices. Although there is no clear evidence on how exactly the hackers penetrated into the system, the attack was likely carried out by a threat actor with the motivation of financial gain or identity theft, and was likely an instance of a targeted phishing attack or a brute force attack on the district's systems. Attack vectors are the methods and techniques used by threat actors to gain unauthorized access to a system or network. (Lemoudden, 2013). The attack vectors may have included exploiting vulnerabilities in the district's software and systems, phishing attacks, and social engineering tactics to gain access to staff members’ credentials.

**Financial/Operational Loss**

The financial and operational losses resulting from the data breach were significant. The district incurred costs related to remediation efforts, including legal fees, credit monitoring services for affected individuals, and other related expenses. The district also experienced reputational damage and a loss of trust from the affected students and staff members. To be more specific, the financial losses resulting from the data breach included the costs associated with the investigation of the attack, remediation efforts to fix the vulnerabilities that allowed the attackers to gain access, and the cost of providing identity theft protection services to those affected. The district spent around $7.5 million to investigate the intrusion, provided identity theft protection services, and upgraded its systems and processes to prevent future incidents. Meanwhile, the operational losses resulting from the data breach were also considerable. The LAUSD accounts for providing education to over 600,000 students, and the data breach disrupted the district's operations and caused extensive delays in providing services to students and employees. The district had to allocate additional resources to prevent the fallout of the data breach, including hiring additional staff members to manage the incident response and remediation efforts.

**Countermeasures**

To mitigate the risk of similar cyber-attacks in the future, the LAUSD could implement a number of technical and tactical solutions. These may include the following:

1. Implementing multifactor authentication to enhance the security of employee credentials and prevent unauthorized access to systems and data.
2. Carrying out security audits and vulnerability assessments to identify and remediate potential weaknesses in the district's software and systems on a regular basis.
3. Providing regular cybersecurity training to employees to ensure that they are aware of the latest threats and best practices for protecting sensitive data.
4. Developing and implementing incident-related dynamic response plans to enable the district to quickly respond to and mitigate cyber-attacks.
5. Investing in updated security technologies and systems, including intrusion detection and prevention systems, firewalls, and antivirus software.

Overall, by taking proactive steps to strengthen its information security posture and implement robust cybersecurity measures, the LAUSD can better protect its students and staff members from the risks of cyber-attacks and data breaches (Bootcamp, 2022).

**Security Risk Management for the LAUSD**

**Overview**

ISO 31000 is a widely recognized international standard for risk management, providing a comprehensive framework for organizations to identify, assess, treat, and monitor risks. The standard offers a systematic approach to risk management and can be applied to a range of organizations, including the Los Angeles Unified School District (LAUSD). By applying this framework, the LAUSD can identify the risks it faces, evaluate their potential impact and likelihood, and develop risk treatment plans that prioritize the most critical risks. In order to establish the context, the LAUSD must define the scope and objectives of its risk management process. This involves identifying the stakeholders, internal and external factors that may impact the risk management process, and the risk criteria that will be used to assess the identified risks. The LAUSD must also consider its risk appetite, or the level of risk it is willing to accept in order to achieve its objectives.

**Proposed risk management framework**

The following is a proposed risk management framework for the LAUSD based on ISO 31000:

1. Establish the context: This involves defining the scope and objectives of the risk management process, as well as identifying the internal and external factors that might influence the district's risk management.
2. Identify risks: This step involves identifying potential risks that the LAUSD may encounter, including cyber threats, natural disasters, human error, and other types of risks. This can be done through a risk assessment process that involves collecting data on potential risks and their likelihood along with overall impact.
3. Analyze risks: This step involves evaluating the identified risks and their potential impact on the LAUSD. This can be conducted through qualitative or quantitative analysis, using tools such as risk matrices, scenario analysis, or cost-benefit analysis.
4. Evaluate risks: This step involves evaluating the identified risks and deciding whether to accept, mitigate, transfer, or avoid them. This can be done by considering the district's risk appetite, legal and regulatory requirements, and other factors.
5. Treat risks: This step involves developing and implementing risk treatment plans to address the identified risks. This may involve implementing controls, procedures, or other measures to reduce the likelihood or impact of the risk.
6. Monitor and review: This step involves monitoring and reviewing the effectiveness of the risk management process and the risk treatment plans. This can be achieved through regular risk assessments, audits, and other monitoring activities.

**Implementation**

To apply this framework to the current risks of the LAUSD, the district would need to conduct a comprehensive risk assessment to identify the specific risks it faces. Based on this assessment, the district could thereafter analyze the risks, assess their likelihood and effect, and determine appropriate risk treatment plans. For example, the district may need to implement stronger cybersecurity measures to protect against cyber threats, such as regularly updating software and conducting regular vulnerability assessments. The district may also need to implement disaster preparation plans to mitigate the impact of natural disasters, such as earthquakes or wildfires.

In general, the ISO 31000 risk management framework can provide the LAUSD with a systematic and comprehensive approach to managing risks, enabling the district to identify potential risks, evaluate their likelihood and impact, and develop and implement effective risk treatment plans to mitigate or prevent them (Priyarsono et al, 2019).

**Adoption of Information Security Framework for the LAUSD**

There are several IT security frameworks that organizations can adopt to manage information security risks. In this response, I will compare and contrast three popular frameworks: ISO 27001, NIST Cybersecurity Framework, and CIS Controls, and then recommend the most suitable framework for the LAUSD and future implications which may occur.

**Three IT security frameworks comparison**

ISO 27001 is a widely recognized international standard that provides a systematic approach to managing information security risks. The framework emphasizes the importance of conducting risk assessments, implementing security controls, and continuously monitoring and improving security performance.

The NIST Cybersecurity Framework is a voluntary framework developed by the US National Institute of Standards and Technology (NIST) that provides a set of guidelines for managing and reducing cybersecurity risk. The framework consists of five core functions: identify, protect, detect, respond, and recover.

The Center for Internet Security (CIS) Controls is a set of 20 prioritized cybersecurity actions developed by a nonprofit organization that offers practical guidance for implementing and improving cybersecurity defenses. The controls cover a range of security areas, including email security, malware defense, and data recovery.

All three frameworks share the common goal of reducing cybersecurity risk, but they differ in their approach and scope. ISO 27001 provides a more comprehensive and structured approach to managing information security risks, while the NIST Cybersecurity Framework is more flexible and adaptable to different types of organizations and risk contexts. The CIS Controls, on the other hand, provide specific, actionable guidance on implementing key security controls (Shinde, 2022).

**The most suitable framework**

In my opinion, ISO 27001 is the most suitable framework for the LAUSD. The framework's emphasis on conducting risk assessments and implementing security controls aligns well with the LAUSD's need to prevent and treat major security risks. Additionally, as a widely recognized international standard, ISO 27001 can provide a clear benchmark for the LAUSD to measure its security performance against.

The LAUSD would benefit from adopting ISO 27001 due to the following reasons:

1. Comprehensive coverage: ISO 27001 provides a comprehensive framework that covers all aspects of information security management, including risk assessment, risk treatment, security controls, and continuous improvement.
2. Global standardization: ISO 27001 is a globally recognized standard, which means that implementing this framework would enable the LAUSD to demonstrate its commitment to information security best practices to stakeholders, such as parents, students, and regulators.
3. Compliance requirements: Many regulations and standards, such as FERPA and HIPAA, require the implementation of information security controls. Implementing ISO 27001 would help the LAUSD meet these compliance requirements.
4. Continuous improvement: ISO 27001 is designed to be a continuous improvement framework. The LAUSD would benefit from this approach because it would enable the district to continually assess and improve its information security posture.

**Future difficulties**

However, there may be challenges in standardizing cybersecurity practices across an organization as large and complex as the LAUSD. Implementing a framework like ISO 27001 requires significant resources and commitment from leadership, as well as ongoing training and awareness-raising for employees. Additionally, the LAUSD may face challenges in integrating security practices across its diverse range of departments and stakeholders.

To summarize the whole section, the ISO 27001 framework is the most suitable framework for the LAUSD to adopt for managing its information security risks. However, standardization in cybersecurity may present some challenges, which the LAUSD will need to address through careful planning, leadership commitment, and ongoing training and awareness-raising.

**Conclusion**

The key findings established from the data breach that occurred at the LAUSD in 2018 include the following:

* The attack was carried out by a group of threat actors who gained access to the district's student information system through a phishing email.
* The attackers were able to steal sensitive personal information of around 500,000 students, including their names, addresses, and social security numbers.
* The LAUSD's information security measures were found to be insufficient, with a lack of proper cybersecurity protocols in place to prevent and detect such attacks.
* The data breach caused significant financial and reputational damage to the LAUSD, with costs estimated to be around $30 million.

The analysis of the data breach identified several factors that contributed to its success, including the attackers' use of social engineering tactics, the LAUSD's inadequate security measures, and the high value of the sensitive personal information held by the district.

To mitigate future security risks, several recommendations were proposed, including implementing stronger security protocols, conducting regular security awareness training for staff and students, establishing incident response plans, and enhancing the district's overall cybersecurity posture through regular risk assessments and audits. Additionally, the adoption of a comprehensive risk management framework, such as ISO 31000, was recommended to help prevent and treat major security risks in the future.

**Reference List**

Alam, M. R., Hasan, M. K., & Rahman, M. S. (2019). Cyber Security Issues in Developing Countries: A Case Study on Bangladesh. IOP Conference Series: Materials Science and Engineering, 598(1), 012107. Available at: <https://iopscience.iop.org/article/10.1088/1757-899X/598/1/012107/pdf> [Accessed 23 Feb. 2023].

Bootcamp, U.C. Berkeley Extension. (2021). Cybersecurity in Education: What Teachers, Parents, and Students Should Know [Blog post]. Berkeley, CA: Bootcamp, U.C. Berkeley Extension. Available at: <https://bootcamp.berkeley.edu/blog/cybersecurity-in-education-what-teachers-parents-and-students-should-know/> [Accessed 17 Feb. 2023].

Educatus Group. (2022). Los Angeles Unified School District. [Website]. Available at: <https://www.educatius.org/schools/usa/los-angeles-unified-school-district> [Accessed 16 Feb. 2023].

Emeritus. (2022). Cybersecurity: What are Cybersecurity Frameworks? [Blog post]. Available at: <https://emeritus.org/blog/cybersecurity-what-are-cybersecurity-frameworks/> [Accessed 22 Feb. 2023].

Rahman, M. S., Islam, M. R., & Bhuiyan, M. Z. A. (2012). Cyber Security: Its Impacts on Rural Society. Journal of Theoretical and Applied Information Technology, 54(2), 226-234. Available at: <http://www.jatit.org/volumes/Vol54No2/15Vol54No2.pdf> [Accessed 20 Feb. 2023].

Sequeira, K. (2015). Hackers Give Los Angeles Unified Monday Deadline. [News article]. Available at: <https://edsource.org/updates/hackers-give-los-angeles-unified-monday-deadline> [Accessed 18 Feb. 2023].