Compliance & Project Management

Individual Project Proposal - Coursework 4

ENHANCING AWARENESS IN CYBER SECURITY:

Boost Cyber Security Posture through User Education

Name: Syed Muhammad Haider Razvi
Student ID: M00832169

CST2531

Table of Contents

1.0 – Title - ENHANCING AWARENESS IN CYBER SECURITY:
Boost Cyber Security Posture through User Education

2.0 – Keywords

- Cyber Security Awareness Training
- Cyber Threats
- Employee Training
- Risk Mitigation
- Data Protection
- Cybersecurity Incidents
- Security Protocols
- Malware Attacks
- Employee Awareness
- Cybersecurity Education

3.0 - Introduction and context description

The Cyber Security Awareness Training website and campaign will educate individuals which will enable the users to understand the basics of Security protocols and its standard operating procedures. This will reduce the human errors that lead to Cyber incidents, which will ultimately reduce the risks of Cyber threats and incidents.

In today's digital world, where technology is at its prime and continues to grow, we have access to a wide range of services and products, including online banking, grocery shopping, payments, electric automobiles, the Internet of Things, online, and more. Artificial intelligence and technological advancements have eliminated every inconvenience that people had to cater with before the development of electronic devices like smartphones, online shopping, e-banking, and other technological innovations. Therefore, along with the benefits of digitalisation, there are many cyber security risks associated with it.

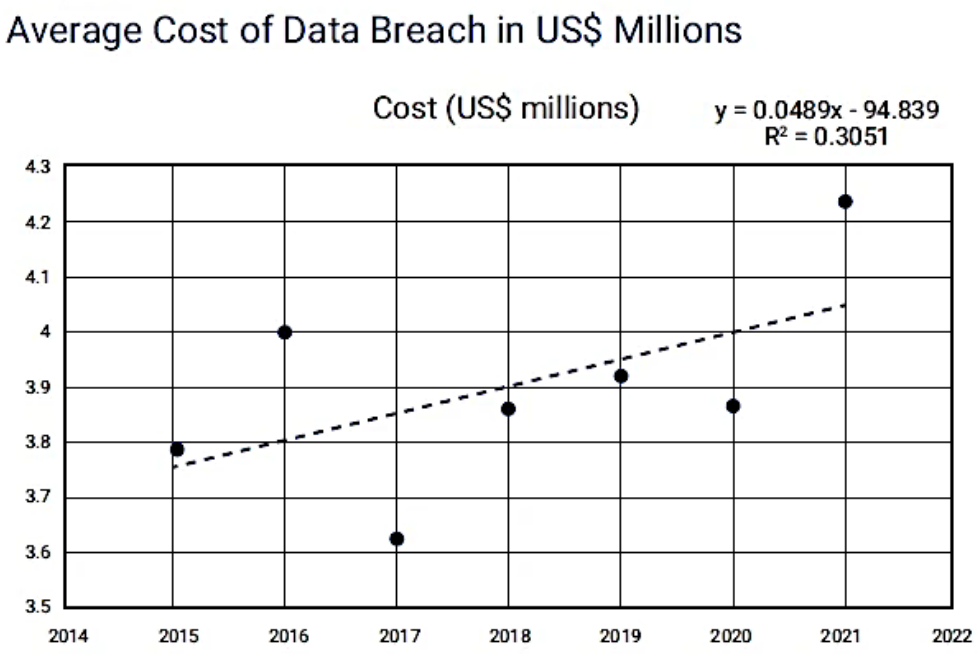
Cybersecurity risks are serious concerns to companies who interact with technology and the internet. The risk is so severe that it can force companies to close their business operations and expose private information about them, including designs, recipes, customer information, and online credit histories. Electronic devices like laptops, and smartphones are also not safe. Therefore, in order to prevent cyber threats and all of these problems, employees as well as consumers of these online services and electronic devices need to be aware of cyber security safety protocols.

This study will highlight the significance and requirement for cyber security training and awareness for workers in online businesses. The goal of this study is to raise user and employee understanding of cyber security issues to shield businesses and people from financial losses, reputational harm, and data breaches. Hackers use new tricks to steal the sensitive data and information of the individuals and organisations, thus, Cyber security awareness, knowledge, and training will empower the users to identify the threats and make smart choices timely.

4.0 - Evidence of requirements

In the Pandemic COVID-19, many companies allowed their employees the convenience of work from home via Zoom, etc. A lot of businesses started operating online and made online websites from which the consumers could shop (European Union Agency for Cyber Security Needs, 2021).

However, during the COVID-19, the cyber-attacks increased, there were 30,000 Cyber-attacks reported in between December 2019 and April 2020, the number of spam messages in between January and April 2020, were 907,000, 737 malware incidents and 48,000 malicious URLS were identified. Moreover, Phishing attacks were enhanced by 220 percent (Fichtenkamm, Burch and Burch, 2022).



The cost of data breach in COVID in 2021 reached to $4.2 million, it shows the costs in 2021 were drastically enhanced as related to those years (Fichtenkamm, Burch and Burch, 2022).

It is reported that in March 2022, the E-commerce business sites grew up by 23% and the expected revenue of online businesses by year 2027 will be $1.7 trillion (Sitelock, 2024).

As a result, organisations and individuals engaged in online operations will encounter an increased number of cyber security threats due to the growing number of online organisations and activities.

The Cyber security awareness and training among individuals and users of the technology is vital to cater with the cyber threats and incidents successfully. This platform of educating and creating cyber security awareness amongst individuals is important as it will highlight the key areas to avoid any online spams, accessing online links, and the users will be aware of the threats and traps the hackers use to extract the online information.

The demand of Cyber security awareness and training platforms have increased by a significant amount of number over the years. It is reported that Cybersecurity awareness training market is expected to grow from $1854.9 million to $12,140 million by 2027. Due to the organisations operating online, the need for cyber security awareness and training for the employees working in the company is necessary to avoid any Cyber related risks (Global Market Estimates Research & Consultants, 2024).

5.0 - Problem identification

The targeted companies in Cyber-attacks in 2023 were Toyota Financial Services (TFS), Yamaha Motor, Google Cloud, UK Royal Family's website, Sony, Discord, State Bank of India, Microsoft, Hyundai, BMW, Paypal, etc (James, 2023).

Even though these businesses employ advanced encryption and cyber security safety measures, they were still targeted in 2023. There is a big chance that employees would be unaware of cyber security safety protocols, which will enable the attackers to easily manipulate staff and launch malware attacks, thus, it is a great risk for the company as the existence of the entire firm will be at risk.

To stop these risks, cyber security awareness training is essential. As you can see, well-known companies like Google Cloud, Paypal, BMW, Yamaha, and Sony are among the 2023 cyber-targets. Due to the Cyber Security Awareness Training platform, workers at organisations will be able to learn about the basics of cyber security and safety protocols, which will prevent from the future Cyber-attacks.

However, relying solely on advanced encryption algorithms and network security protocols is not the only way to prevent cyber-attacks and hackers. Therefore, the problem identified is that companies should emphasize on the need of investing into the Cyber Security Awareness & Training programs as well to avoid any sort of Cyber and malware attacks. This will eradicate the chances of human errors as the employees will be well informed in the basic security principles of the cyber security, as a result, the hackers will not be able to manipulate them by sending malicious links or emails.

6.0 – Aims

Information Technology, and Artificial intelligence are dominating the world. So, there are significant risks associated with advanced technology. Our platform's aim is to create cyber security awareness and provide them with training in order to reduce this risk.

The cyber security awareness and training platform's aims emphasize on a better understanding of cyber security protocols and principles to eliminate the cyber security threats. The aims are to ultimately reduce the cyber security incidents, and to create a safe and secure internet environment.

It will focus on educating employees about cyber security threats that might jeopardise both the organisation and their personal sensitive information.

The platform for cyber security awareness and training has several significant aims, which are:

- **Risk Mitigation:** Long-term benefits to the company will result from raising employee awareness of potential cyber threats and teaching them how to recognise them. This will reduce the likelihood of human error because employees will know exactly what to do and will refrain from actions that could put the company at risk.

- **Improved security structure:** The cyber security awareness and training campaigns will allow the employees to develop skills in the basics of cyber security safety protocols, which will enhance the security-conscious culture in the working environment of the company, which will ultimately lead to a stronger security structure. Thus, this will benefit the business in long term as positive working culture will be promoted.

- **Protect the sensitive and classified information:** The platform assists in the protection of the company's data assets by training employees on the value of protecting sensitive information and best methods for doing so. In future, it will prevent the hackers from hacking the company's valuable data and information as employees will be well informed and trained.

- **Adjusting to new and evolving security risks:** Cyberthreats are constantly modified. A training platform guarantees that employees remain updated on the newest methods and trends employed by hackers. Up to date security strategies will always disable hackers from illegal intrusion and stealing company's data in the long term.

- **Ready to respond to cyber incident:** Employees will benefit from cyber security awareness and training, which will provide them with a clear picture of what to do in the event of a cyber security crisis. This will prevent significant losses for the company and enable workers to react to an attack quickly incase of any cyber incident or attack.

7.0 – Objectives

To achieve the cyber security awareness and training platform's broader aims, it will be divided into achievable short-term targets or objectives, which can be measured easily, are time restrictive, and achievable (Wadhwa, 2023).

Cyber security training and awareness aims can be achieved by;

- **On-the field training for employees:** Conduct regular cyber security workshops for employees and educate them about the significance of creating strong passwords, multi-factor authentication. Moreover, address them about the malware attacks, how are they occurred and how to avoid them.

- **Off-the field training for employees**: is when the training to the employee is provided outside the work premises and company. It means that our platform will also provide certificates and short courses in cyber security. Employees can select from a wide range of our online cyber security short courses, which are, foundations of cyber security, introduction to cybersecurity fundamentals, introduction to cyber security tools and cyber attacks.

- **Promote Multimedia content:** Educate the employees and individuals in a fun way, by showing them the animated pictures, videos, slides, and infographics.

- **Safe use of social media:** Informing workers regarding the cyber threats by using social media, including controlling their online footprints, excessive sharing, and fraudulent accounts (LinkedIn, N.D.).

- **Interactive Learning Modules:** To promote learning and active engagement, provide engaging sections that include exercises, tests, and real-world scenarios (LinkedIn, N.D.).

- **Cloud security:** Explaining workforce members about the secure cloud computing techniques and methods (LinkedIn, N.D.).

- **Train how to use emails properly:** Educate employees about phishing and malware, and assist them in detecting fraudulent messages (Nationwide, n.d.).

8.0 - Methods chosen for project implementation

i. Website

Website will be created of Cyber security awareness and training, on which, employees and users can read the blogs, and articles about Cyber security fundamentals, and cyber security basic security protocols for free.

Moreover, paid short courses for Cyber security will also be offered on the website and will be given with a certificate upon the completion of the short course. The website is created using HTML, CSS, Javascript, Node.js, and My SQL for database. It allows users to pay via debit/credit card on the website to access the short courses. The website meets the Payment Card Industry Data Security Standard (PCI DSS) requirements to protect cardholder data.

Encryption methods like AES-256-bit encryption/decryption algorithm have been used to encrypt sensitive data of the users accessing the website.

ii. Canva

Canva is used to create videos and images related to cyber security. It made it possible to create slideshows, movies, templates, and pictures to meet multimedia demands.

9.0 – Brief Product Description

A website-based cyber security awareness training platform is an online resource that teaches users about different cyber threats along with efficient practices. The platform is convenient and available from any device with internet connectivity.

This platform usually provides a variety of cyber oriented blogs, articles, videos, quizzes, and cyber security short courses. Users can move through the course at their own speed and can get performance feedback.

Furthermore, website-based cyber security training programmes provides features like performance monitoring and certificates upon completion of short courses. The aim is to make consumers more conscious of the significance of cyber security and provide them with the necessary skills.

10.0 – Deliverables

- A fully functional Cyber security awareness Website.
- Interactive lessons on various cyber security topics
- Multimedia content for engaging learning
- Quizzes and Assessments: Tests to evaluate knowledge
- Monitoring users' completion and performance
- Certifications: Recognition for completing modules successfully
- Reporting and Analytics: Data-driven insights into user engagement and effectiveness
- Assistance for technical issues or questions

11.0 - Outcome/product evaluation/testing approach

1. **Usability Testing:** Make sure the platform is user-friendly and intuitive by evaluating its UI/UX design.

2. **Security Assessment:** Conduct regular security checks to avoid any cyber threats.

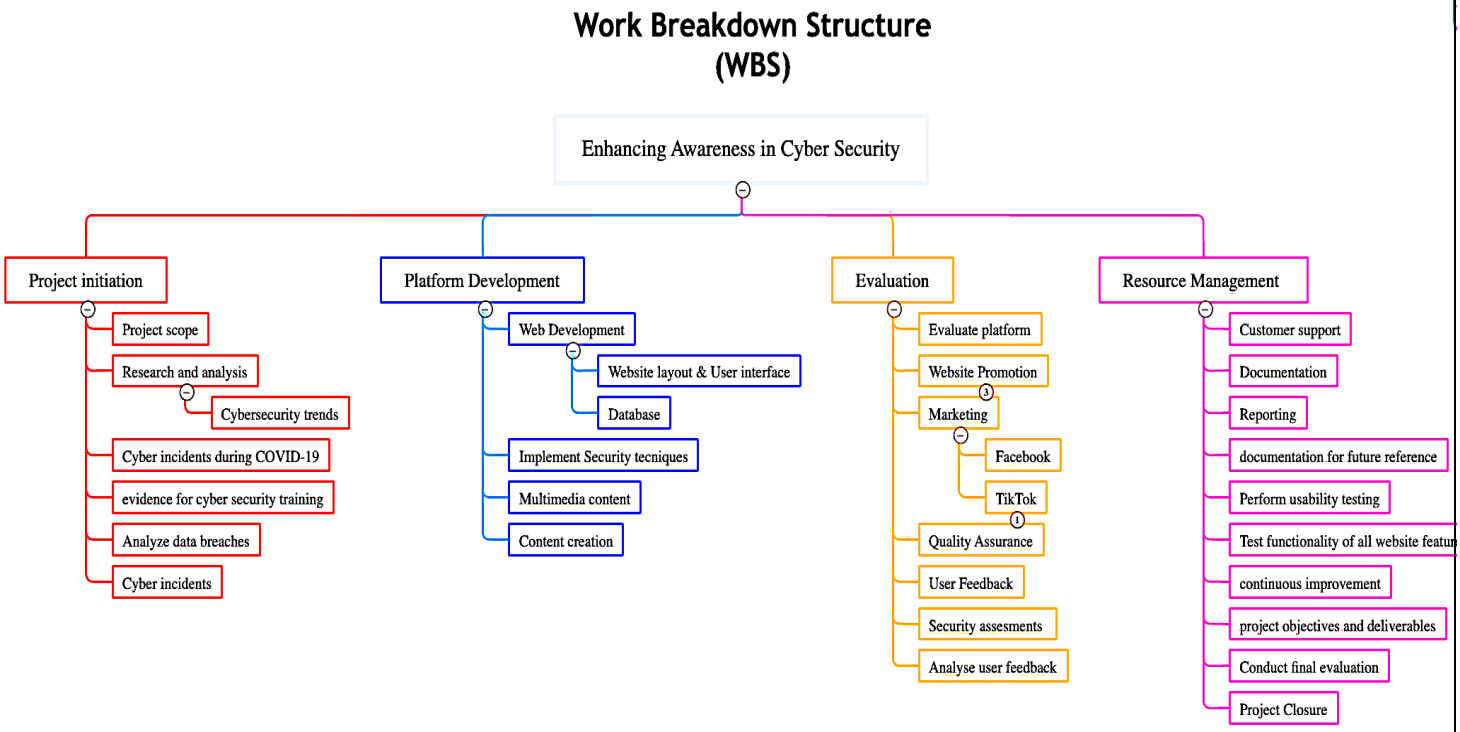
3. **Functionality Testing:** Ensure all the functions of the website including, online quizzes, videos, tests, database, and payment systems works.

4. **User feedback:** Consider the feedback of the consumers to highlight the areas of improvement.

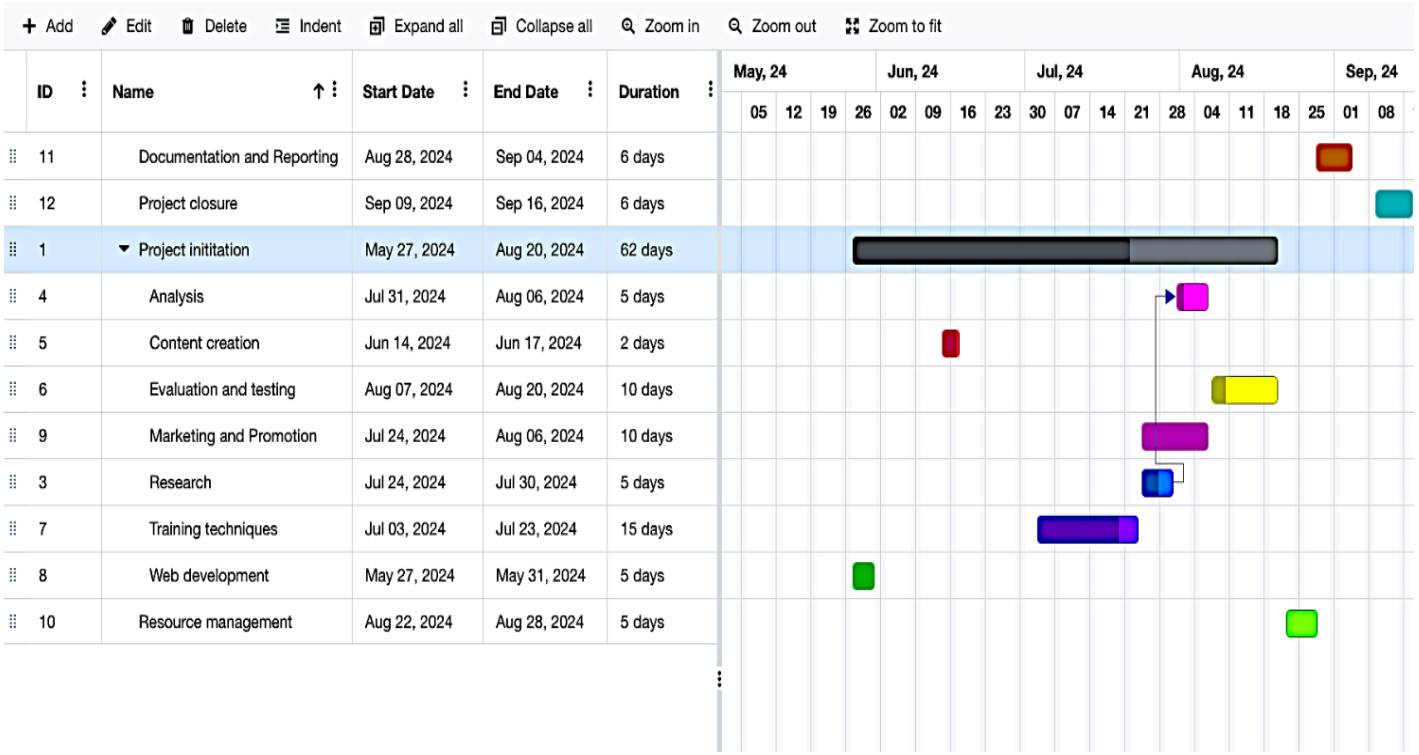
12.0 – Resources

- Website was built using HTML, CSS, JavaScript, My SQL, Node.JS.
- Canva was used for videos, images, graphs, and infographics.
- Social media platforms like Facebook, TikTok, and Instagram were used to promote the website and our campaign.
- Emails were sent to various companies to introduce our compaign and website in their company.

13.0 – Work Breakdown Chart



14.0 – Gantt chart



5. 0 - Reference List

Fichtenkamm, M., Burch, G.F. and Burch, J. (2022). Cybersecurity in a COVID-19 World. [online] ISACA. Available at: https://www.isaca.org/resources/isaca-journal/issues/2022/volume-2/cybersecurity-in-a-covid-19-world [Accessed 8th Apr. 2024].

Sitelock. (2024). Most Common Cyberattacks on eCommerce Websites. [online] SiteLock. Available at: https://www.sitelock.com/resources/ecommerce-guide/impact-of-security-incidents-to-your-ecommerce-business/ [Accessed 8th Apr. 2024].

Global Market Estimates Research & Consultants. (2024). Global Cybersecurity Awareness Training Market Analysis. [online] Available at: https://www.globalmarketestimates.com/market-report/cybersecurity-awareness-training-market-3669 [Accessed 8th Apr. 2024].

James, N. (2023). Recent Cyber Attacks - 2023 - Astra Security Blog. [online] Available at: https://www.getastra.com/blog/security-audit/recent-cyber-attacks/ [Accessed 8th Apr. 2024].

'Cybersecurity guide for SMEs, 12 steps to securing your business'. (2021) European Union Agency for Cyber Security Needs, Page 2-10. Available at: ENISA%20Cybersecurity%20guide%20for%20SMEs-online-single_page.pdf [Accessed 8th Apr. 2024].

Wadhwa, P. (2023). Top Three Cyber Security Goals. [online] Sprinto. Available at: https://sprinto.com/blog/cyber-security-goals/ [Accessed 8th Apr. 2024].

Nationwide. (n.d.). *How to Train Employees on Cybersecurity - Nationwide*. [online] Available at: https://www.nationwide.com/business/solutions-center/cybersecurity/train-employees [Accessed 8th Apr. 2024].

Linkedin. (n.d.). What are the objectives of cyber security awareness? [online] Available at: https://www.linkedin.com/pulse/what-objectives-cyber-security-awareness-thesecurityco [Accessed 8th Apr. 2024].