MITIGATING DATA BREACHES BY IMPROVING SITUATIONAL AWARENESS

HAZAR HISHAM AKBAR

CYBERSECURITY PROGRAMME

SCHOOL OF COMPUTER SCIENCE AND INFORMATICS

CARDIFF UNIVERSITY

November 2021

Mitigating Data Breaches by Improving Situational Awareness

Author

Hazar Akbar

A dissertation submitted in partial fulfillment of

the requirements for the degree of:

Master of Cybersecurity

Supervisor

Neetesh Saxena

Cybersecurity Programme

School of Computer Science and Informatics

Cardiff University

November 2021

Declaration of Originality

I hereby declare that this dissertation report is based on my original work except for citations and quotations, which are duly acknowledged. I also declare that this report has not been previously and concurrently submitted for any other degree or award at Cardiff or other institutions.

Acknowledgment

First of all, I would like to begin by expressing my profound appreciation to Allah and thank him that he gave me the power to complete my master's degree and finalize this dissertation specially we were facing COVID-19 time.

From the deepest part in my heart, I would want to express my gratitude to my country, the Kingdom of Saudi Arabia, and its Cultural Bureau in the United Kingdom, for giving me the opportunity and supporting me financially to complete my master's degree at Cardiff University in cybersecurity field. I also would like to thank my supervisor in Saudi Cultural Bureau Mr. Hassan Ghannam as he was with me in every time that I need help or support.

My dissertation was a big opportunity to obtain practical and theoretical experience. It was made possible thanks to the assist of my supervisor Dr. Neetesh. I would like to present my deepest gratitude and thanks to him for his unlimited support, and guidance throughout the dissertation that made the result more successful. Completing this program was my academic aim. However, this would not have been possible without the assist of so many at Cardiff University. I would like to Thank Prof. Omer Rana, Dr. Amir Javed, Dr. George Theodorakopoulos, Dr. Philipp Reinecke, and Dr. Shancang Li for their professionalism throughout the studying period.

I have to express my appreciation to my family. Thanks to Mrs. Mawahib Samman, my lifelong teacher, my mother, and my every beautiful thing in my life for being next to me and attend to all my needs. Thanks to Mr. Hisham Akbar, my father and role model in my life. Thanks to Mr. Rayan Alharbi, my best friend, and wonderful husband for encouraging me and believing in me while pursuing higher education and all other successful in my life. Thanks to my sisters; Abrar and Lamar, and my brother Hamid. Thanks to my kids Sulaf and Abdulaziz. I would like to say that I would not have achieved my goals without you being them with me. Thank you all. I love you all.

Abstract

These days, cybersecurity has gained implicit importance because the number of cybersecurity threats continues to increase. This is due to the rapid growth of using technology in all aspects of life. Dependency on such technology prompts users to provide their sensitive information in order to perform their work and achieve their needs. The digitalisation of data is resulting in an increase in the incidence of cybercrime. Data breaches are considered one of the most dangerous consequences of cybercrime. In previous studies, a wide range of countermeasures have been discussed. Notably, improving situational awareness has delivered positive results. To mitigate data breaches, we set a list of security requirements for organisations to meet as well as proposing a tool that is based on improving cyber situational awareness. Numerous requirements have been proposed for the tool but we implemented one function of these requirements which is reflecting the password situation. The current research applies a qualitative method and through experiments, we reflected on the password situation regarding GUI. We show that visualising the situation makes users more aware of what happens around them. Furthermore, our experiment results also show that visualising the situation using colour coding makes users categorise and understand situations.

Key words: Data breach, Situational Awareness.

Table of Contents

List of Figures *8*

List of Tables *9*

List of List of Abbreviations and Acronyms *10*

Chapter 1: Introduction *11*

1.1 Research motivation **11**

1.2 Research statement **12**

1.3 Research aim and objective **13**

1.4 Research impact **13**

1.5 Target audience **14**

1.6 Organisation of the current study **14**

Chapter 2: Background and literature review *15*

2.1 Overview **15**

2.2 Data breach background **15**

2.2.1 What is a data breach? 15

2.2.2 Data breach phases 16

2.2.3 General workflow of data breach 17

2.2.4 Data breach consequences 18

2.2.5 Data breach incident cases 18

2.2.6 Data breach countermeasures 21

2.3 Situational awareness **25**

2.3.1 What is situational awareness? 25

2.3.2 Who needs situation awareness? 27

2.3.3 How to obtain situation awareness? 27

2.3.4 The importance of cyber situational awareness 28

2.4 Literature review **29**

2.5 Key findings **34**

2.6 Summary **35**

Chapter 3: Methodology *36*

3.1 Overview **36**

3.2 Research approach **36**

3.3 The approach to develop the tool **37**

3.3.1 Spiral model overview 37

3.3.2 Situational awareness tool development phases 38

3.3.3 Dataset collection ... 39
3.4 Results and evaluation approach ... 39
3.5 Summary ... 39
Chapter 4: Design and Implementation ... 40
4.1 Overview ... 40
4.2 Application of the proposed tool in the real-world ... 40
4.3 The tool requirements ... 41
4.3.1 Functional requirements ... 41
4.3.2 Non-functional requirements ... 48
4.4 Design ... 48
4.4.1 Initial graphical user interfaces (GUI) design ... 48
4.4.2 Password requirements ... 49
4.4.3 Situational awareness colour coding ... 49
4.5 Implementation ... 50
4.5.1 Implementation of requirement 1 (check password strength) ... 50
4.5.2 Pseudocode of requirement 1 (check password strength) ... 51
4.6 The experiment ... 54
4.7 Environment setup ... 54
4.8 Dataset description ... 54
4.9 Summary ... 55
Chapter 5: Results and Evaluation ... 56
5.1 Overview ... 56
5.2 Result ... 56
5.2.1 Security requirements ... 56
5.2.2 The experiment results ... 60
5.3 Evaluation ... 63
5.4 Summary ... 65
Chapter 6: Conclusion ... 66
6.1 Limitations and future work ... 66
Reflection on Learning ... 68
References ... 69
Appendix A ... 74
Appendix B ... 83

List of Figures

Figure 1: General breach workflow for data breaches according to Saleem and Naveed (2020). 17
Figure 2: Dissertation methodology 36
Figure 3: Use Case Diagram 46
Figure 4: The initial design of requirement 1 (check password strength) page. 49
Figure 5: The final design of requirement 1 (check password strength) page. 51
Figure 6: Result when choosing the 000webhost dataset 60
Figure 7: Result when choosing the hak5 dataset 61
Figure 8: Result when choosing the izmy dataset 62
Figure 9: Result when choosing the Lizard-Squad dataset 63
Figure 10: The initial design of requirement 2: employees report page 83
Figure 11: The initial design of requirement 3: assets report page 83
Figure 12: The initial design of requirement 4: track asset page 84
Figure 13: The initial design of requirement 6: assets management page 84
Figure 14: The initial design of requirement 6: assets management page (add) 85
Figure 15: The initial design of requirement 7: View National Cyber Security Centre Tweets.....85
Figure 16: The initial design of requirement 8: task reminders page 86
Figure 17: The initial design of requirement 11: tasks management page 86
Figure 18: The initial design of requirement 11: tasks management (add) 87
Figure 19: The initial design of appearing the tool on the organizations' homepage. 87

List of Tables

Table 1: Data breach incident cases 21
Table 2: The importance of applying SA in various fields 30
Table 3: The latest detection and prevention techniques that deal with data breaches 32
Table 4: Non-functional requirements of our tool 48
Table 5: Datasets details 54
Table 6: The needed security requirements for businesses to be secure 57
Table 7: Estimated processing time 64

List of Abbreviations and Acronyms

Acronym	Definition
SA	Situational Awareness
IDS	Intrusion detection systems
IPS	Intrusion prevention systems
DLPS	Data leakage prevention systems
GUI	Graphical user interface
GDPR	General Data Protection Regulation
SMEs	Small and medium-sized enterprises
MoSCoW	Must, should, could and would

Chapter 1: Introduction

Cybersecurity has become increasingly significant over time on account of the growing number of threats. This is due to the rapid rollout of technology in various fields of life. Rapid advances in technology and frequent use of the Internet have made many individuals, businesses and organisations dependent on these channels because they provide convenience, speed and many other benefits. As a result of relying on this digital world, however, users are required to provide personal details such as their name, phone number and email address when working, shopping and socialising in order to achieve their needs and process their work (Fang et al. 2019). The digitalisation of data is leading to an increase in instances of cybercrime. Hackers are becoming more advanced and they are targeting more diverse sectors in public and private communities (Adlakha et al. 2019). Therefore, it is essential to better protect data because it is not surprising that attackers will seek to take advantage of data being digitalised or being transmitted online by stealing it. This kind of personal data leakage is utilised for credit card fraud at the individual and institutional levels (Fang et al. 2019).

1.1 Research motivation

Despite all of the efforts made to fight cyber-crime, recent statistics published by Enisa state that data breaches pose a considerable threat that affects daily life and they announced that data breaches were considered one of the 10 top threats over the period from January 2019 to April 2020, maintaining the same status as in 2018 (ENISA 2020a). They also reported that the number of breaches has been increased by 54% during 2019 compared to the previous year. They also clarified that the motivation for data breaches was financial in 71% of cases (ENISA 2020b). For these reasons, and because of the passive consequences they could have on the victims, there is a clear need to reduce the number of breaches.

On the other hand, according to Cheng et al. (2017), it has been noticed that many researchers focus on detecting and preventing data leaks. The aim of their studies is to prevent data from leaking and detecting attempts to commit cybercrime. These types of solutions have a positive effect on the detection and prevention of data breaches within companies. However, the ability to raise situational awareness to reduce the number of data breach incidents in the first place is important for the organisation's information security. Therefore, the main motive of the current study is to improve situational cyber awareness to minimise the consequences of such incidents.

1.2 Research statement

Data breach stories are still trending on the news every day. Even with the many existing solutions to help manage cyber-attacks and the many state-of-the-art techniques used to detect and prevent data breaches, these solutions alone could be inefficient at responding to attacks that leads to data breaches. In addition, these solutions might cost organisations considerable sums to protect their confidential data, thereby potentially jeopardising the sustainability of the underlying business.

It might be due to a lack of cyber situational awareness. As Adlakha et al. (2019) stated, a lack of awareness is a major factor behind the significant rise in cybercrime. In addition, according to Raulerson (2013), to have a perfect defence in cyberspace, the cyber defenders must have sufficient situational awareness of their environment. Thus, even with many solutions in place, the issue is complicated because of an unawareness of the whole picture. This constitutes a limitation because the need here is to increase situational awareness to make people aware of the whole picture and see the issue from different perspectives in order to reduce the possibility of breaches.

To bridge this gap, a tool needs to be developed that can increase situational awareness because solutions related to increased awareness could potentially be appropriate. More specifically, the current study sets out to answer the following questions:

- Do data breaches still have a significant impact even with the existing solutions in place?
- Does the increase in situational awareness help mitigate data breaches?
- Do weak passwords lead to data breaches?

1.3 Research aim and objective

The current study aims to develop a novel tool that could make the security administrator aware of the cyber situation in organisations. To achieve this aim, three objectives have been defined:

1. List the security requirements needed to prevent data breaches.
2. Develop a tool that: 1) reflects the password situation regarding whether they have recently been updated and are sufficiently strong; 2) reflect the asset situation regarding whether they are updated and their locations; and 3) remind the security administrator of important security tasks to improve cyber situational awareness.

1.4 Research impact

The importance of the current study stems from the need to apply cyber situational awareness or increase it as a model in the security field. The importance of the current study includes scientific and practical aspects:

1. Scientific importance: It provides an academic scientific benefit because the results will increase interest in the situational awareness and contribute to the scientific research literature. The results of the current study may provide a strong incentive to carry out complementary studies or to replicate the same study in other environments.
2. Practical importance: The results of the current study are expected to help those interested in and concerned with the matter by providing results and recommendations. In addition, in various institutions, the importance of this dissertation derives from the fact that it may encourage them to apply situational awareness, if only in a simple way to achieve its benefits and reduce the risk of data breaches or errors that lead to data breaches.

1.5 Target audience

Because one of the research objectives is to develop a tool capable of improving situational awareness, the study focuses on cyber security companies and software developing companies to adopt the idea and improve such tool capabilities to serve the security area.

1.6 Organisation of the current study

In addition to this introductory chapter, the report contains six chapters, each of which focuses on one aspect of implementing the tool that improves situational awareness in the field of cybersecurity. More specifically, **Chapter 2** presents a general understanding of the data breach issue, explains its general workflow, discusses the available countermeasure and their consequences, and provides details of some past data breach incidents and their consequences. It then clarifies the meaning of situational awareness. At the end of this chapter, the related work is presented. **Chapter 3** presents the selected study methodology along with the adopted framework for developing the tool. **Chapter 4** provides details of the tool design and how it will be developed and implemented, whilst **Chapter 5** outlines the needed security requirements and results of the evaluation after developing the tool. Finally, **Chapter 6** concludes the dissertation with a summary of what has been achieved, as well as discussing the limitations and making recommendations for future work.

Chapter 2: Background and literature review

2.1 Overview

To make this report understandable, it is necessary to clarify some important knowledge relating to data breaches and cyber situational awareness. This chapter discusses two main fields: a) the background to data breaches and situational awareness; and b) a literature review of previous studies that have been carried out in these areas. It starts by providing a general understanding of data breaches, stating their phases and general workflow, discussing the consequences, identifying some notable data breach incidents, and stating some of the available countermeasures. In addition, it explains in detail the meaning of situational awareness and then discusses its importance in cyberspace. Finally, the previous related works to this dissertation are presented.

2.2 Data breach background

The following sections describe data breaches in detail, including their definition, phases and general workflow, the possible consequences, several cases of previous data breaches, and some of the existing countermeasures.

2.2.1 What is a data breach?

Businesses of all sizes have been interested in the concept of data breaches recently as they have become significantly reliant on the digital world, workforce mobility, and cloud computing. Due to the reliance on storing data in databases, cloud servers and local machines, increasing attempts are being made to leak organisations' data. However, data breaches have been attempted throughout history, before companies relied on technology and storing sensitive information digitally. Indeed, such attempts were made when individuals and enterprises stored

their private information in written records. In the past, however, data breaches would typically occur when unauthorised people found and viewed sensitive printed documents that were not disposed of properly.

According to Hart (2016), a data breach is a type of security compromise that involves the use, viewing or theft of protected, confidential or sensitive data that could be stored on a system, database or printed materials by an unauthorised individual without knowledge of the data owners or without their permission. This data could contain personally identifiable information (PII), private health information (PHI), private credit information (PCI), trade secrets, intellectual property or any information that could be important to the enterprise or others.

2.2.2 Data breach phases

Extracting data usually entails three phases which are the research phase, the attack phase, and the exfiltrate phase:

- **First Phase: Research** involves the attackers searching for weaknesses or gaps in the organisations' security, including devices, networks, systems and employees. This could involve many hours of searching by the attacker. For example, attackers may search social media profiles to gain insight into the organisation's infrastructure and then perform a social engineering attack against those employees who have privileged access to systems in the organisations.
- **Second Phase: Attack** means the attackers gain a foothold in the company's network or the security perimeter after making initial contact via a network-based or social-based attack.
- **Third Phase: Exfiltration** is the final phase. It involves the attackers successfully extracting data from the network of the victim organisations and then using this sensitive and confidential data for personal gain such as reselling it on the black market, cyber propaganda, blackmail to demand a ransom, or performing additional damaging attacks on the infrastructure of their target (Adlakha et al. 2019; Imperva 2021; Trend Micro 2021).

2.2.3 General workflow of data breach

Saleem and Naveed (2020) summarised a general workflow of a data breach after studying 10 cases of data breach incidents step-by-step in detail and briefly reviewing a further 50 data breach incidents.

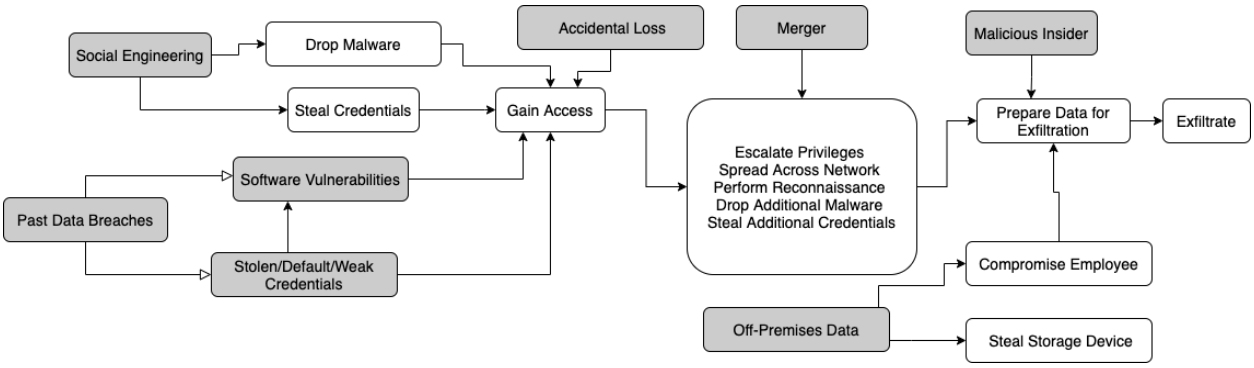

Figure 1: General breach workflow for data breaches according to Saleem and Naveed (2020).

To make Figure 1 more understandable, this section provides some explanations.

- **Off-premises data.** This refers to when employees take their laptops or important data beyond their work boundary. In a worst case scenario, these devices or data are then stolen from the employees. In addition, it refers to when employees export data to their personal devices or upload it to the cloud. Then they are vulnerable to successful phishing attacks that could enable attackers to steal credentials which would compromise the data too.
- **Accidental loss.** This refers to employees accidentally disclosing the organisation's data; for example, sending information to the wrong email address or keeping the database public on the Internet.
- **Mergers**. This refers to the fact that some companies suffer data breaches without being aware that they have been compromised and it is only after they merge with other companies that the breach is discovered.
- **Social engineering.** This refers to when employees experience a successful spear-phishing or phishing attack. Thus, they enable attackers to compromise a company’s network and then access sensitive data or even install a backdoor.

- **Software vulnerabilities.** This refers to when employees ignore warnings to update software and they ignore the requirement to restart devices after updates have been made.

2.2.4 Data breach consequences

Data breaches continue to trend around the world, despite data security becoming more important. Attackers are increasingly becoming experts at finding new ways to gain access to valuable data. They try each available trick to penetrate, expose and profit from sensitive data, whether it is by planting malware, supply chain attacks, or using sophisticated social engineering techniques. According to ENISA's Data Breach Report (2020b), the total number of breaches increased by 54% in 2019 compared with the number in 2018 and approximately three in four breaches were financially motivated. The consequences of data breaches go beyond the financial losses. Some of the more harmful consequences of this issue include:

- Intellectual property theft.
- Damage to the organisation's reputation.
- Adversely affecting people's lives because it can in some cases lead to divorce, suicide or death when it discloses information about their health records or their personal life.
- Disclosure of confidential information which might in the future be used for blackmail.
- Making organisations face legal bounds when they fail to protect data according to General Data Protection Regulation (GDPR).

Despite some of these consequences being dependent on others, all of them will affect the finances and reputations of the target organisations, potentially causing the closure of businesses, particularly small and medium-sized enterprises (SMEs).

2.2.5 Data breach incident cases

Unfortunately, there are very few published studies that explain data breach incidents, the workflow of the breach, and the reasons that led to the breach. This might be because, as stated by Stewart (2009), many enterprises are still reluctant to announce that they have experienced data breaches because they are afraid of harm being caused to their reputation as well as the

associated clear-up costs. However, this section discusses two incidents in depth, including the causes, impacts and costs of five incidents (see Table 1).

- **Target 2013**

In 2013, according to Shu et al. (2017), the retailer 'Target' suffered a data breach when the attacker stole 70 million pieces of personal information and 40 million credit and debit card numbers. The breach cost Target $162 million.

How did the breach start? First of all, Target did not discover the breach themselves. Instead, they were alerted by the Justice Department. The breach started when the attacker sent a phishing email to one of Target's third-parties, namely Fazio Mechanical. The employee of Fazio had been infected with a Citadel Trojan which uses web injects to alter the HTML of the targeted websites on the victim's side (victim's computer) to add fake forms that ask for credentials and sensitive information in the context of websites that look like a real website. In addition, this trojan tends to record screens to steal credentials and capture screenshots. Using this trojan, the attacker stole the credentials of Fazio's employee on Target's vendor web service. Then the hacker logged into the web portal of Target using the stolen credentials. After that, they used the upload function to upload a PHP web-shell and because there was not sufficient security to check the validity of the file types, it was uploaded successfully. The uploaded PHP web shell enabled the hacker to remotely access the Target web server. Then the hacker located critical areas such as the point-of-sale terminals and database servers as well as escalating the privilege to connect with network hosts without requiring a password. While accessing these hosts, the hacker found a host with an admin account, retrieved the password hash of the admin and then utilised it to create a new admin account to imitate the admin account. After creating a new admin account, the hacker used it to reach the database server and point of sale (POS) terminals. Subsequently, Microsoft's SQL tools were used to retrieve data for 70 million Target customers. Because Target was compliant with the Payment Card Industry Data Security Standard (PCI-DSS), the database did not have any information regarding customers' payment cards. The security team at Target ignored the alerts that came from the detection system when it recognised intruder activity, thereby helping the hacker to deploy on Target's POS terminals a customised version of Black-

POS malware. This malware was utilised to retrieve payment card information when the memory interacted with the card reader. The stolen data were then stored in a shared file that was created on a FTP along with stolen copied data from the local files from the database server. The breached data consisted of 70 million records that included the names, phone numbers and mailing addresses of customers. In addition, 40 million payment card records were obtained, including the card holder's name, card numbers, dates of expiration, and (CVV) card verification values (ibid).

- **Yahoo 2014**

In 2014, Yahoo suffered a data breach when an attacker stole account information for more than 500 million users. In addition, the hacker created forged authentication cookies to obtain access to the email accounts of various Russian journalists, private-sector employees, and Russian and US government officials. The hacker also turned the traffic on Yahoo's search engine to other websites to achieve monetary profit as well as selling the stolen accounts on the dark web. The breach cost Yahoo $4.48 billion (Saleem and Naveed 2020).

How did the breach start? The hacker stole the credentials of Yahoo employees by sending spear-phishing emails to them and making them visit phishing sites. After having obtained their credentials, they used these to access the network of Yahoo remotely and then install a backdoor to enable them to gain access continually. The hacker escalated the privilege of other hosts and then spread across the network. It was not known what the precise techniques was but the hacker used key-loggers to steal credentials. Then the hacker found a database of Yahoo users and a management tool to reach and edit the database. The database contained information such as names, email addresses, hashed passwords, password recovery emails, dates of birth, security questions and answers, and cryptographic nonces unique to each account. The hackers took advantage to exfiltrate a backup of the database containing over 500 million records by using the File Transfer Protocol (FTP) as well as using the management tool to recognise the accounts of various Russian journalists, private-sector employees, and Russian and US government officials by utilising the password recovery email address from the database. However, the management tool did not permit searches to be made on the database using the

victims' names. In some situations, the domain of the non-Yahoo email account offered a hint about the user's company. Moreover, in order to generate cash, the hacker turned the traffic of Yahoo's search engine to an online pharmacy which paid for the traffic. Ultimately, to avoid detection, the hacker used log cleaning tools to clear the event logs (ibid).

Table 1: Data breach incident cases

Source	Companies	Causes	Impact	Cost
GAO (2018)	Equifax 2017	Occurred because there was an application vulnerability	147.9 million consumers	Unknow
Adlakha et al. (2019)	Adult Friend Finder 2016	Occurred because there was a weak SHA1 hashing algorithm	More than 412.2 million accounts	Unknow
Holm and Mackenzie (2014)	eBay 2014	Occurred because of the poor implementation of the password renewal procedure and a lack of communication with users	145 million users compromised	Unknow
Adlakha et al. (2019)	Heartland Payment Systems 2008	Vulnerability to SQL injection, thus malware was planted on the network	34 million credit cards exposed	$145 million as compensation
Adlakha et al. (2019)	TJX company, Inc 2006	Weak data encryption	94 million credit cards exposed	$200 million

2.2.6 Data breach countermeasures

The following section discusses and lists some of the existing solutions and techniques that have been used to fight data breaches. In order to improve understanding, the countermeasures are divided as technical or non-technical.

2.2.6.1 Technical

- **Firewalls**

  Sampaio and Bernardino (2017) stated that the firewall is a software-based or hardware-based network security device that uses a rule set to regulate incoming and outgoing network traffic. It establishes a partition between the internal network (trusted secure) and another external network such as the internet. In other words, it is a system designed to deny unauthorised access and unauthorised data outflows from reaching local or internal devices. Firewalls can be set up to protect the boundary of an organisation and segment the network to edge from the hackers' lateral movement. Also, firewalls can be used to block any unwanted network traffic such as preventing employees from uploading private information to the internet or accessing malicious webs pages (Roozbahani and Azad 2015).

- **Intrusion detection system and intrusion prevention systems**

  Intrusion detection systems (IDS) are used to monitor network traffic from any suspicious activity or illegal access by unauthorised users and then alert the system administrator of any suspicious activity discovered. Intrusion prevention systems (IPS) are similar to an IDS but the difference is that the IPS can be configured to block potential threats. Both are used to discover attackers when they attempt to use social engineering techniques, install malware, escalate privilege or communicate with command-and-control servers. Thus, IDS are used to detect attempted attacks and IPS are used to block such attempts (Roozbahani and Azad 2015).

- **Data leakage prevention systems**

  Data leakage prevention systems (DLPS) is a system that is used to identify, monitor, protect and reduce the danger of sensitive data being leaked. It is used to detect and prevent unauthorised individuals from accessing sensitive data as well as being used to protect confidential data that could be shared accidentally (Tahboub and Saleh 2014).

- **Anti-malware**

  This refers to any software that protects computer devices and systems from malware such as spyware, viruses or other malicious programs. The purpose of anti-malware software is to work in the environment in real-time. However, it only looks for external threats by scanning and validating the signature in order to ensure that the infection is removed from malware (Tahboub and Saleh 2014).

- **Multi-factor authentication**

  This is an electronic authentication method whereby the user is permitted access a website or an application only after submitting two or more factors or pieces of evidence successfully. It is a step designed to protect systems against strangers because the traditional log-in methods based on a username and password are not fully protected against attackers because they could guess the credentials using certain tools. Multi-factor authentication could be divided into two methods: two-factor authentication and authentication based on biometrics. Two-factor authentication is based on sending one-time passwords to a mobile telephone number or to an email address; however, iris, retina, fingerprint and face recognition are examples of authentication based on biometrics (Alsaleem and Alshoshan 202).

- **Encryption**

  This is a mechanism that is used to encrypt data into ciphertext in order to secure the data against being disclosed. The encryption process entails translating data into unreadable information using an algorithm. Thus, when authorised, individuals are able to access the data and they may try to read it by decrypting using a key. This technique is vital for organisations to protect their sensitive information against being breached (Raigoza and Jituri 2016).

2.2.6.2 Non-technical

- **Staff training and education**

  Zamosky (2014) confirmed that the greatest information security threat that companies face tends to be from their own employees, regardless of how a data breach occurs. This is because some employees simply do not follow the companies' policies and procedures. In a survey conducted in 2013 by Forrester Research, Zamosky found that the misuse of data by employees came at the top of a list of breach causes. Meanwhile, the same study found that 58 per cent of employees did not undergo any training on how to stay secure at work and the study reported that approximately 60% of employees do not know anything about their companies' security policies. As a result, Zamosky emphasised the need for companies to put in place their own policies and procedures and they must ensure that their staff receive sufficient training to know what their policies and procedures are. In addition, research conducted by Rastenis et al. (2019) showed that educated individuals are not immune to phishing attempts that could lead to data breaches and there is no link between being academically educated and being educated in terms of security fields.

- **Policies**

  Stewart (2009) confirmed that applying security policies helps prevent many breaches from happening. In addition, he confirmed that whilst many organisations have polices in place, their staff or management often fail to follow these polices. He mentioned that according to Verizon, 59% of data breaches occur not because they did not have security policies and procedures but because these measures were not implemented.

There is further discussion regarding state-of-the-art detection and prevention techniques for data breaches in Section C of the literature review.

2.3 Situational awareness

Situation awareness (SA) is becoming a notable aim for those who would like to improve operator interfaces, training programmes, and automation concepts in many different fields (Endsley and Garland 2000). There has been a considerable increase in attention paid to SA since the mid-1980s (Endsley and Garland 2000). They clarified that many factors influence SA, the most important of which are the challenges posed by a new class of technology.

SA has always been required for individuals to accomplish activities properly because people need to be aware of many indications in their environment. For a long time, having perfect SA was essentially a question of experience and training, as well as learning the key signs to watch out for and what they indicate. However, with new life patterns, the focus turned to developing a new class of tools to help individuals perform tasks. The existing tools are no-longer simple; they are incredibly complicated and focus on perceptual and cognitive tasks in detail in addition to the physical tasks. Many people in various fields must perceive and comprehend data that frequently varies very quickly which could present a challenging information gap (ibid).

Modern systems are able to produce a large quantity of data and can provide information on almost anything, anytime and anywhere on the planet. However, the issue with systems is not a lack of information but obtaining what is required at the time it is required. Many individuals sadly might be less knowledgeable to face this deluge of data. This is due to a big gap between the data produced, the spread of data and people's capacity to find and understand data in order to make their decisions. As a result, the standards that people expect from system designs have shifted. Moreover, to implement systems that give people the required capabilities and information, it has to be delivered in a way that is useable physically and cognitively (ibid).

2.3.1 What is situational awareness?

SA is commonly defined in a way that has proven to be applicable over a board range of fields. According to Endsley and Garland (2000), it is "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of

their status in the near future." To explain, individuals do not have to be aware of everything but they have to know and understand the most significant information that relates to their goal. SA is divided into three levels: perception, comprehension and projection.

- **The first level of SA is perception** which is the knowledge that reflects the environment's operational picture. It is the result of collecting raw information from activities such as sensing the environment, receiving messages about it or interacting with it. It is essential to note that the individual does not combine essential elements of the raw information to infer meaning. The fundamental perception of the main information affects the likelihood of forming a correct picture of the situation (Ahmad et al. 2021).
- **The second level of the SA is comprehension** which encompasses how people merge, explain, retain and hold information. As such, it is more than perceiving the information, rather, it is a combination of multiple information parts that determine the relevant individual's aims. It is like understanding the whole paragraph after reading instead of just reading the words. It is the result of linking the raw information collected to form a full picture of the situation. Individuals with the comprehension level have been able to obtain the relevant meaning from the perception level (ibid).
- **The third and highest level of SA - projection** is a result of extrapolating from the current mental model that helps to generate alternative system states and environment states in the future. It is the ability to forecast future case events and understand the situation carefully to make decisions. Endsley and Garland (2000) stated that in each field they studied, they had found that experts rely heavily on future projections. Decision-making is supported by the projections because the individual evaluates the case and interprets the future scenario in the field of the objectives as a foundation for decision-making in the future (Ahmad et al. 2021).

2.3.2 Who needs situation awareness?

The complex increase in automation and electronic systems has prompted searches for the latest tools and methodological frameworks to efficiently handle domain changes. However, it must be stated clearly that electronic systems themselves do not give SA. It depends on human understanding to make the information useful. The need for SA has always existed, regardless of how the individual performs their work, even in fields that are not traditionally thought to be very cognitive or technological. The emphasis on having SA in the existing design of systems is due to: a) assistance in providing perfect SA via decision aids and system interfaces; b) individuals are able to hinder SA via the same efforts if they fail to meet their SA needs adequately (Endsley and Garland 2000).

2.3.3 How to obtain situation awareness?

Signals could be received via visual, olfactory, auditory, tactile or taste receptors. Some signals may be subtle, such as changes to an engine, whilst some may be public such as an alarm system. Due to the shift into remote operators' instantiation in numerous domains, the main challenge could be giving enough information via the remote interface compensating for the signals when immediately perceived.

It is essential to observe that whereas designers of the system tend to concentrate on the provided information via the systems and the interfaces, that is not considered the sole source of SA. In various fields, individuals might be able to watch and listen directly to information from the environment itself, but in some scenarios that might not be the case. Therefore, it is essential to take into account the SA given by system designs and the information that individuals obtain from other sources. This concerns what is the added value by a specific system taking into consideration what one can already acquire from other sources and how much it might cost in terms of interference with this information?

Additionally, to instantly perceive information, the sensors of systems gather several subsets of accessible information that is available from the environment and the internal parameters of

systems. A subset of the data held by the system is presented to individuals via their user interface. With this information, individuals understand and interpret certain parts, thereby resulting in SA.

It is important to remember that this is not a passive procedure to obtain displayed information; rather, the individuals might be very actively involved. For example, individuals in different systems could take control to display information. They may also be capable, for example, of controlling what information the system gathers by sending commands out to obtain definite information from connected systems or by covering the sensors and setting the paths. People are thus highly active volunteers in the situation assessment procedure, with SA leading the procedure and the procedure resulting in SA (ibid).

2.3.4 The importance of cyber situational awareness

Cyberspace is a continually improving and changing environment with new threats, threat actors, vulnerabilities and other factors appearing on a daily basis. The need to have and improve SA has grown as activities have expanded and reliance on cyberspace has grown. Enterprises can identify, recognise, process, and grasp information in real-time thanks to SA which gives both a holistic and specific picture of threats and weaknesses. In addition, SA allows for an accurate perception of the organisation's security posture and the threat environment. As a result, organisations can better assess their existing and future risk status as well as their security posture (Cyware 2018).

Humans are the weakest link in cybersecurity and SA solves this problem. It helps reduce the likelihood of human error that results in damage. Indeed, SA has grown in importance in the information security field, allowing enterprises to develop internal threat intelligence sharing channels that warn all-important workers about emerging threats, mitigations, and possible scenarios of attacks. Enterprises can benefit from SA by understanding in a better way what is going on in cyberspace and their environment. In addition, SA can help incident response teams

to make educated decisions about how best to guard against and respond to possible threats (ibid).

2.4 Literature review

Having a comprehensive understanding of data breach dimensions can lead to the implementation of perfect solutions. The detailed literature review addresses the foundation for answering the research questions. In order to provide the necessary information, this section presents the empirical literature concerning four perspectives: A) Data breaches issues; B) Situational awareness; C) Existing techniques for detecting and preventing data breaches; and D) The result of applying weak passwords.

A) Data breaches issues. The impact of data breaches is still an issue that faces many organisations. **Joseph (2017)** examined the scope of data leaks and their occurrences in the public sector in the US by analysing data breaches over a period of five-years from 2011 to 2015. He stated that data breaches are not a new trend because in the past, breaches happened even data was stored on paper-based records. He added that personally identifiable information (PII) is the most valuable data for criminals and stated that the average cost in 2015 of a single data breach was $3.8 million and the majority of these incidents go undetected for 160 to 240 days. **Teymourloueiand and Harris (2018)** discussed data breaches and the associated costs as well as the vulnerability and methodology to minimise risk. They considered data breaches to pose a significant risk because they affect identity and financial information. They mentioned that successful breaches have grown year-on-year from an average of 102 to 130 (more than 27%). **Karunakaran et al. (2018)** noted that data exposed by breaches represents a significant risk to Internet users and they suggested that best practice for responding to breaches is still lacking. They conducted two surveys to examine data breaches risk and the sentiment of 551 participants towards possible remediation steps. In addition, they asked 10,212 participants to rate their comfort level with eight different scenarios. **Fang et al. (2019)** clarified that in recent years, underground forums have played a key role in the trading and sharing of exposed personal information as well as being used as information sources about data breaches. The authors

presented a system that automatically detects threats that are linked to data breaches in real-time. **Adlakha et al. (2019)** emphasised the need to have a comprehensive understanding of cyber-attacks, classify them, and know how to be secure against them. In addition, they discussed data breaches and the various types that have happened in the past.

B) Situational awareness. Having SA in place is an important phenomenon in the cyber security field and also in other fields. Table 2 presents details of the empirical literature that has discussed the importance of applying SA in various fields.

Table 2: The importance of applying SA in various fields

Author(s)	Study field	Synopsis
Nagaria and Hall (2020)	Technology	An experiment was conducted on 10 software developers that involved training them online and the authors concluded by stating that maintaining SA could reduce human errors in many different domains.
Collinsa et al. (2020)	Sport	SA is a vital safety aspect in guided sea kayaking trips because it affects the decisions made by guides. After conducting an experiment, the key findings suggested that the guides' understanding and recognition of fundamental informational cues lacked both comprehension of the meaning and the capacity to project the future effect on the situation. It was recommended that sea kayaking guide training needs to instil a sound comprehension of the situations that guides might experience as well as an ability to predict the possible effects of those situations.
Rizzo (2018)	Management	In the leadership literature, SA has emerged as an important phenomenon. In order to make educated decisions, leaders and followers in all settings should be acutely aware of their surroundings. The fundamentals of SA are the obligation to apprehend the truth for the moment, sighting with supervision and cautiously considering possibilities.
Calder et al. (2018)	Healthcare (emergency)	Participants working in emergency resuscitation teams believed that displaying SA has the potential to enhance the performance of the provider and communication of the team, thereby resulting in improved care quality.
Fore and Sculli (2013)	Healthcare (nursing)	Successful perception, comprehension, and/or projection could dramatically increase the accuracy, appropriateness and adequacy of

		patient-care decisions. Therefore, as a precursor to decision-making, poor or inadequate levels of SA present serious threats to patient safety. Thus, as a decision-making introduction, levels of SA should be high and adequate to prevent serious threats to patient safety. It has been recommended that SA should be examined in the theoretical context and studied systematically because it is an essential factor in providing safe patient care.
Malu et al. (2012)	Business	The high number of existing unstructured data adversely affects enterprises. As a result, it has been recommended that there should be a real-time capability to correlate and analyse unstructured data that flows from many different sources to enable companies to be aware of external events that could impact their business operations. Thus, SA affords managers the opportunity to make operational decisions in the necessary time before it is too late.
Endsley (1999)	Aviation	Maintaining SA is an important and difficult aspect of the job of aircrew. Even the best-trained staff can make terrible decisions if they lack SA. The goal of maintaining a high level of SA at all times is difficult due to several factors that are a constant elements of the aviation environment. The main issue for aviation research over the next decade will be to improve SA through better cockpit design and training programmes. Ultimately, there is a need for high SA in the aviation sector.

In addition to the numerous studies that discuss SA in various fields, there are many studies that recommended developing a cyber SA model or tool. In this direction, **Atif et al. (2021)** provided a process model which explains how organisations could practice SA in the threat landscape. They also improved the information processing network and demonstrated how to control the information flow to achieve better SA. They recommended that organisations improve SA in their incident response practices. **Mayer et al. (2021)** confirmed that there is a limited realisation of human awareness in their response to data breaches that affect them. They conducted an experiment that led them to confirm that there is a need for user-friendly tools to improve SA against breaches and to mitigate them. **Okolica et al. (2009)** presented a framework to better understand SA in the cyber field. They concluded by recommending that a cyber SA model be developed that aims to build an automated discovery engine for commanders at different levels to give an actionable and helpful picture of cyber SA.

C) Techniques for detecting and preventing data breaches. Many different attacks that result in data breaches have threatened organisations in various sectors as well as individuals over the years. Consequently, there is a plethora of studies addressing the topic of data breach countermeasures. Various solutions have been developed and improved. Table 3 presents details of the empirical literature that discusses the most innovative detection and prevention techniques that deal with data breaches.

Table 3: The latest detection and prevention techniques that deal with data breaches

Author(s)	Technique	Advantages
Liu et al. (2020)	Artificial intelligence	• Maximise the security of sensitive information storage • Minimise the risk of data leakage
Shapira et al. (2013)	Fingerprinting	Simple strong approach
Hart et al. (2011)	Machine learning	High accuracy algorithm
Papadimitriou and Molina (2010)	Watermarking	Help forensic analysts to identify leakers
Bertino et al. (2005)	Analysis of user behaviour	• Protection against insider threats • Usable for databases with a large user population
Spitzner et al. (2003)	Honeypots	Discover malicious insiders

Liu et al. (2020) proposed a prevention technique based on artificial intelligence that involved studying the existing data breach prevention technology and they designed a data asset leak prevention system to deal with the changing and complicated network threat situation. **Shapira et al. (2013)** stated that fingerprinting is a method applied to detect data leaks. To detect the leaking of sensitive content using the fingerprinting technique, the signatures of known confidential content are retrieved and compared to outgoing content. They proposed an extension approach to fingerprinting that relies on sorted k-skip-n-grams. The approach makes a fingerprint the core sensitive content whilst ignoring non-relevant parts. Moreover, the proposed approach is better able to rephrase and could be applied to detect a previously unnoticed private document which means it can provide perfect intentional leak detection. **Hart et al. (2011)** developed accurate machine learning algorithms to distinguish sensitive from non-sensitive data

and classify the documents in organisations based on whether they are structured or unstructured documents as either public or private. **Papadimitriou and Molina (2010)** reported on the watermarking technique which is utilised to detect and prevent data leakage by making a mark on the data when distributed. Thus, if a distributed copy is discovered in an unauthorised party's hand, the forensic analyst could identify who leaked the information. They discussed the difficulty of identifying responsible parties in the event of data breaches and then proposed data allocation strategies that increase the likelihood of detecting leaks. **Bertino et al. (2005)** suggested a model to analyse users' database access behaviours to discover any anomalous access patterns by strangers or insiders and detect data leaks based on mining database traces saved in log files in relational databases. This technique identifies users who access database systems and knows their role because users playing a given role act in a specific way that differs from the normal role behaviour. **Spitzner et al. (2003)** discussed honeypot technology and proposed employing it to discover insider threats at an early stage. The idea was to apply it to the network by inserting honeytokens with perceived value. After that, these honeytokens might direct insiders to the advanced honeypots and determine whether or not their intention was malicious.

D) The result of applying weak passwords. Using weak passwords might lead to a data breach. **Rajah et al. (2020)** confirmed that individuals usually use weak passwords in order to remember them, such as the date of their birthday for numerical passwords or relying on simple words. They clarified that poor password habits put personal data at risk and enable hackers to gain unauthorised access to these passwords and deploy cyber-attacks. In addition, they emphasised the need to apply second-factor authentication across accounts. Meanwhile, **Keszthelyi (2013)** estimated that approximately 80% of data breaches result from the use of weak passwords that can be guessed. **Matthews (2012)** stated that having a password is not enough to defend against hackers who use methods that are designed to exploit password vulnerabilities. Matthews also emphasised the need for strong passwords and second-factor authentication to create a high level of security.

2.5 Key findings

The main conclusion drawn from the previous research is that despite all of the efforts made to tackle data breaches using the existing solutions and techniques to detect or prevent them, data breaches are still trending in the news headlines as well as affecting companies and billions of users, resulting in severe consequences and impacting even the best-resourced organisation, thereby indicating that the available solutions need to be improved. It is notable that the existing solutions to detect and prevent data breaches depend on technology itself taking action rather than relying collaboration between technology and humans to give them a better understanding and enable them to take appropriate decisions to prevent data breaches.

There are many studies in different sectors which have confirmed that increasing SA has yielded promising results. According to Kokkonen and Puuska (2018), the objective of SA in the cybersecurity field is to be aware of what the security level is and what the security level of the organisation's assets will be in their networked systems. Moreover, in some studies, researchers have recommended increasing cyber SA to achieve a better understanding and to make sound decisions to protect valued assets in the most accurate and swift way. Meanwhile, the review of studies in Section D discusses the consequences of applying weak passwords. Moreover, according to Bonneau et al. (2012), although various alternative approaches to authentication have been presented in recent decades, the most prevalent form for securing access to computer systems and network services remains text-based passwords. Thus, they confirmed that this authentication is unlikely to be replaced in the near future due to its comparative advantages of simplicity, convenience and low cost.

Thus, to bridge the gap, we propose developing a tool based on improving SA which could play a significant role in terms of improving the results to help mitigate data breaches. The proposed tool will be implemented and integrated with organisations' systems. The tool will be for the security administrators who are responsible for monitoring security in the information technology department of the organisation to make appropriate decisions depending on the situation faced. The proposed tool will provide a visual interpretation regarding the passwords'

level of compliance as well as other features. More information regarding the tool features is provided in Chapter 4. The proposed tool offers the potential to extend the abilities of the current security technologies that already exist because it is considered an additional technology to monitor and react to changing situations and circumstances in real-time.

The findings of this report should help companies that develop software as well as cybersecurity companies to improve their tools' capabilities by incorporating SA. The main contribution of the current study is to ensure humans are aware of what is happening around them in order to minimise the negative impact of cyber-attacks, especially data breaches. In addition, to the best of the writer's knowledge, no study has previously suggested or provided a tool integrated with existing systems to increase cyber SA regarding passwords.

2.6 Summary

The issue of data breaches has been considered one of the main cyber threats for several decades. The consequences of this issue go beyond financial loss and can ruin successful companies. Consequently, considerable empirical literature has been undertaken in the field of data breaches, providing insight into the definition, impact and solutions from the perspective of detection and prevention. Stewart (2009) stated that data breaches are inescapable and, for this reason, he added that it is vital for organisations' executives at all levels to understand the impacts and the consequences of data breaches and be ready for the inevitable. Understanding and planning could reduce the pressure when breaches are discovered and will make it more likely that efforts to mitigate will succeed. It is apparent that researchers from various fields have focused on improving the understanding of SA to realise better results and conclusions. The proposed solution is based on making humans actively participate in efforts to mitigate data breaches and ensure they are aware of what is going on around them.

Chapter 3: Methodology

3.1 Overview

The object of this chapter is to demonstrate in detail the methodology that has been applied to conduct the current study. The methodology is divided into three sections. The first section discusses the approach that has been taken to achieve the stated research aim and objectives. The second section discusses the approach to develop the tool because the findings recommend developing a tool. The third section explains how the results and evaluations will be conducted.

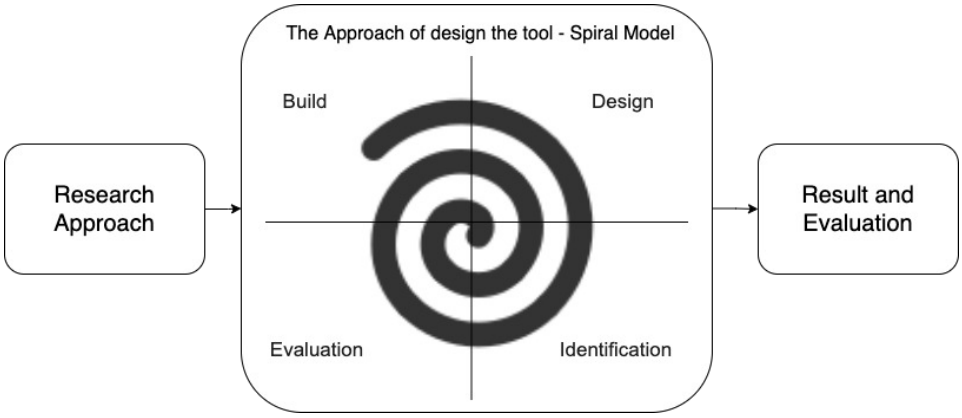

Figure 2: Dissertation methodology

3.2 Research approach

The design of the research is intended to provide an adequate framework. A considerable element of the research design concerns the choice to be made regarding the research approach because it determines how the related information will be obtained from various sources. The research uses a qualitative method to address the different fundamental objectives of the

research as well as to expand the knowledge, consider the different perspectives of other researchers and build on the current knowledge.

A comprehensive search has been carried out to understand the problem, analyse it and arrive at the best solution whilst answering the stated research questions. This entails a comprehensive review of the empirical literature gathered via Google Scholar, IEEE Xplore Digital Library, Research Gate, Science Direct, and Cardiff University Library. The review contained several reputable articles and journals as well as cybersecurity companies' websites and their channels on YouTube such as Enisa, McAfee, FireEye, and SANS. The information concerned data breach issues, the results of applying SA in many different sectors, discussing the existing solutions and the innovative techniques available to detect and prevent data breaches and determine whether applying weak passwords could lead to data breaches.

3.3 The approach to develop the tool

After concluding the research section and understanding the problem, the recommendation was to build a tool based on improving situational cyber awareness. To achieve this aim, it was deemed that the Spiral model was the most suitable approach because of its flexibility in allowing changes to the requirements to add greater functionality later.

3.3.1 Spiral model overview

This is one of the software development methodologies. It is a combination of iterative development and the waterfall model. This model allows for incremental product releases or enhancement as each iteration around the spiral progresses. The Spiral has four phases which are the identification phase, design phase, construct or build phase, and evaluation phase (Satzinger and John 2016).

3.3.2 Situational awareness tool development phases

- **Identification phase**

In this phase, the tool requirements (functional and non-functional) have been set based on answers to the dissertation questions as well as being based on our reading and knowledge of some of the reasons for data breaches. Thus, there was a desire to build a tool that could help to increase awareness regarding the situation with passwords in organisations along with the situation regarding organisations' employees' passwords and organisations' assets. The requirements of the tool will be prioritised in accordance with the MoSCoW methodology in order to prioritise the requirements when developing software (Agile Business Consortium 2021). This is discussed further in Chapter 4.

- **Design phase**

After establishing the functional and non-functional requirements, it is essential to model the requirements in specific diagrams. To design the recommended tool, we opted to utilise use cases and give a detailed explanation as well as opting to draw graphical user interfaces to visualise the interfaces. We used diagrams.net to draw the use case diagram and proto.io to draw the interfaces. diagrams.net is an open-source tool for developing diagramming applications (diagrams.net 2021). proto.io is an online diagram platform -free 14 trial - for high-fidelity screens GUI (proto.io 2021). A more detailed discussion regarding the design phase is given in Chapter 4.

- **Construct/build phase**

According to the use MoSCoW methodology, the implementation would only be for the first tool requirement due to the time allocated to complete this dissertation. The proposed tool must be integrated with the organisations' systems and we did not seek this option because our tool proposal must access sensitive information in the organisations to measure the strength of the passwords and then reflect the situation to ensure that the security administrators are aware of what is happening around them. Thus, it is difficult to ask any organisation to give us permission to access their sensitive data. Therefore, we implemented the tool and reflected on the situation based on measuring the strength of passwords in password datasets that we found using the

Google Dataset search engine. More information regarding the environment setup and the implementation is presented in Chapter 4.

- **Evaluation phase**

We discuss our methodology of the evaluation phase in Section 3.4.

3.3.3 Dataset collection

To build our SA tool, it was important to have a collection of passwords. This was necessary to test the performance of our tool. In order to create appropriate selection options, we used the Google search engine and the Google Dataset search engine. We searched using the following keywords: “passwords dataset,” “passwords,” and “passwords list.” We found a public account on the GitHub website, namely SecLists. This account has a collection of numerous datasets (Miessler 2021). Regarding the specific choice of the datasets, we chose four at random but focused on selecting datasets that varied in terms of the record numbers.

3.4 Results and evaluation approach

After concluding the research section and finishing designing and implementing our proposed tool, Chapter 5 presents a list of the security requirements needed to prevent data breaches with along with a discussion of how such a SA tool could help these requirements. In addition, it presents an evaluation of how our tool performs after testing it via using four datasets.

3.5 Summary

This chapter has illustrated the overall path of the dissertation. The dissertation has indicated different methodologies that have been conducted in this research. The methodology has been divided into three parts which are the research part, the developing tool part, and the results and evaluation part.

Chapter 4: Design and Implementation

4.1 Overview

Despite having advanced technologies to prevent data breaches, the number of incidents is increasing. To help mitigate this increase, it has been recommended to build a tool based on improving SA. This chapter discusses the proposed tool and its requirements, before explaining the design and its implementation. It starts by giving an overview of the application of the proposed tool in the real world and then discusses the functional and non-functional requirements of the tool. Subsequently, the initial graphical user interface of the tool is presented and there is a discussion of the password standard requirements and the colour-coding of SA. This is followed by a detailed explanation of the building phase of the tool. The final sections provide details of the environmental setup and the datasets used in this experiment.

4.2 Application of the proposed tool in the real-world

The proposed tool is assumed to be integrated with the organisation's systems. Thus, the implementation of this tool requires access to the organisation's databases to process the results based on their data. It is assumed that the data have been decoded before being passed to the tool. The data will be used to visualise the existing situation in the organisation to raise the SA of the security administrator. Section 4.3.1 presents a more detailed explanation of the tool functionality.

4.3 The tool requirements

The tool will be web-based; thus, it will work on PCs, laptops, tablets and smartphones that run the Windows or macOS operating systems and have an internet browser. This section discusses the functional and non-functional requirements.

4.3.1 Functional requirements

The functional requirements of the tool are categorised according to the MoSCoW methodology. The first functional requirement is based on answering one of the stated research questions, while the rest of the requirements have been set according to the writer's knowledge of some of the reasons that lead to data breaches. Thus, it has been focused to increase awareness of what happens around us. In addition, this section displays the use case diagram of the proposed tool functional requirements with an accompanying description.

4.3.1.1 MoSCoW methodology

Must Have

Requirement 1: Check password strength

Awareness of the security level of the passwords in an organisation is essential to reduce the possibility of a breach. The tool enables the security administrator to be aware of the employees' password security level according to specific standards and then visualise the result on the screen without disclosing any information about them. The specific measurement standards of the passwords are discussed in Section 4.4.2 password requirements standards of the tool

Should Have

Requirement 2: Employees' report

Updating passwords regularly is considered one of the best practices that can help minimise the number of breaches. Regarding this matter, the tool allows the security administrator to be aware of when employees updated their passwords. Thus, the tool displays a table containing information about the organisation's employees. The information includes their name, title, phone number, email, the date when they last updated their password, and the security level.

The security level displays a colour coding to visualise whether the password has been updated recently or has been used for a while. To make this clear, it is assumed that the measurement will be on a three-month basis, thus:

- If the password has been updated within the date range 0-45 days: the colour will be green, which signifies a normal situation.
- If the password has been updated in the date range 46-90) days: the colour will be amber, which signifies a middle situation.
- If the password has not been updated within the previous 91 days: the colour will be red, which signifies an abnormal situation.

As a result, this function enables the security administrator to make an appropriate decision regarding each employee when necessary.

Note:

- The measurement of this function could be set as the security administrator desires, whether three months is the default, less or more.
- The result will appear based on comparing the saved dates for updating passwords in the database.

Requirement 3: Asset report

Updating software regularly is essential to reduce the likelihood of experiencing a breach. It may be necessary to remind the security administrator to perform this task. Regarding this matter, the tool will issue a reminder which allows the security administrator to see a table displaying information about the organisation's assets such as PCs, security devices, printers, IoT devices, and so on. The information about these assets will include the model names, model numbers, software, last update dates, reminder dates, and tracking information. The tracking information will appear as a button and when the user clicks on the button, the asset tracking page will appear. An explanation of the tracking is provided in requirement 4: Track assets.

As a result, this function enables the security administrator to be aware of the devices and their last update date, thus he makes the right decision regarding updating the software.

Note. It is assumed that the data in this table has been completed by the security administrator and saved in the organisation's database. A detailed of managing assets function is provided in requirement 6, requirement 9, and requirement 10.

Requirement 4: Track asset

Losing devices and theft is one of the causes of data breaches. Thus, knowing the location of the devices could help to find them as soon as they are lost. To enable the security administrator to be aware of the devices' locations, the tool allows the security administrator to track devices and view them on a map. The devices will be visualised on the map according to a colour-coding and details of the colour-coding are provided in Section 4.4.3. As a result, this function enables the security administrator to be aware of the devices' locations.

Note. It is assumed that the information about devices' locations is compiled by the security administrator and saved in the organisation's database. A detailed of managing assets function is provided in requirement 6, requirement 9, and requirement 10. The devices must have a tracking SIM in order to connect and perform this function.

Requirement 5: Alert

The tool alerts the security administrator when a situation arises. The notifications appear on the tool's notification page and are sent by the tool to the administrator's email account. The situations that trigger an alert are as follows:

- When it is time to update devices.
- When it is time for to perform tasks
- If any device is taken far away from the organisation's boundary.

As a result, this function enables the security administrator to be reminded of important dates as well as enabling them to be aware of what is happening around them so that they can make appropriate decisions.

Note. The necessary data to perform this function is assumed to be saved in the organisation's database.

Could Have

Requirement 6: Asset management (Add asset)

In order to perform requirement 3 (assets report), requirement 4 (track asset) and requirement 5 (alert), the tool allows the security administrator to manage the organisation's assets by adding, updating and deleting assets. Assets are added by filling out a form with the device information including its model name, model number, software, last update date, reminder date, and tracking information.

Requirement 7: View National Cyber Security Centre Tweets

Being aware of the latest important news or information regarding cybersecurity is vital for the security administrator. The tool allows the security administrator to read the latest tweets from the National Cyber Security Centre account on Twitter.

Note. One or more Twitter account can be selected to follow as the security administrator desires.

Requirement 7: Task reminders

To perform the security risk assessment and the penetration tests regularly and analyse the existing security policies regularly to suggest improvements, it is recommended to set reminders for the security administrator. The tool allows the security administrator to set memos to remind them to perform their security tasks.

Note. It is assumed that the information in this table has been filled in by the security administrator and saved in the organisation's database. A detailed of managing tasks function is provided in requirement 11.

Won't Have

Requirement 9: Asset management (Update asset)

In order to perform requirement 3 (assets report), requirement 4 (track asset) and requirement 5 (alert), the tool allows the security administrator to manage the organisation's assets by adding,

updating and deleting assets. Asset updating is performed by choosing a device from the registered devices, opening its form and updating its information before pressing submit.

Requirement 10: Asset management (Delet asset)

In order to perform requirement 3 (assets report), requirement 4 (track asset) and requirement 5 (alert), the tool allows the security administrator to manage the organisation's assets by adding, updating and deleting assets. Asset deleting is performed by choosing a device from the registered devices, opening its form and then pressing delete.

Requirement 11: Task management (Add task)

In order to perform requirement 7 (task reminders), the tool allows the security administrator to manage their tasks by adding, editing and deleting tasks. The task will be added by filling out a form with the task name, task detail and task reminder date.

Requirement 12: Task management (Edit task)

In order to perform requirement 7 (task reminders), the tool allows the security administrator to manage their tasks by adding, editing and deleting tasks. The task is edited by choosing a task from the registered tasks, opening its form and then updating its information before pressing submit.

Requirement 13: Task management (Delete task)

In order to perform requirement 7 (task reminders), the tool allows the security administrator to manage their tasks by adding, editing and deleting tasks. The task is deleted by choosing a task from the registered tasks, opening its form and then pressing delete.

Requirement 14: Sign-in

The tool is integrated with the organisation's system which means that in order to use it, the security administrator must be authenticated and via the organisation's system dashboard, the security administrator chooses the SA tool button.

Requirement 15: Sign-out

The tool allows the security administrator to log out and clear the cookie session.

4.3.1.2 Use Case Diagram

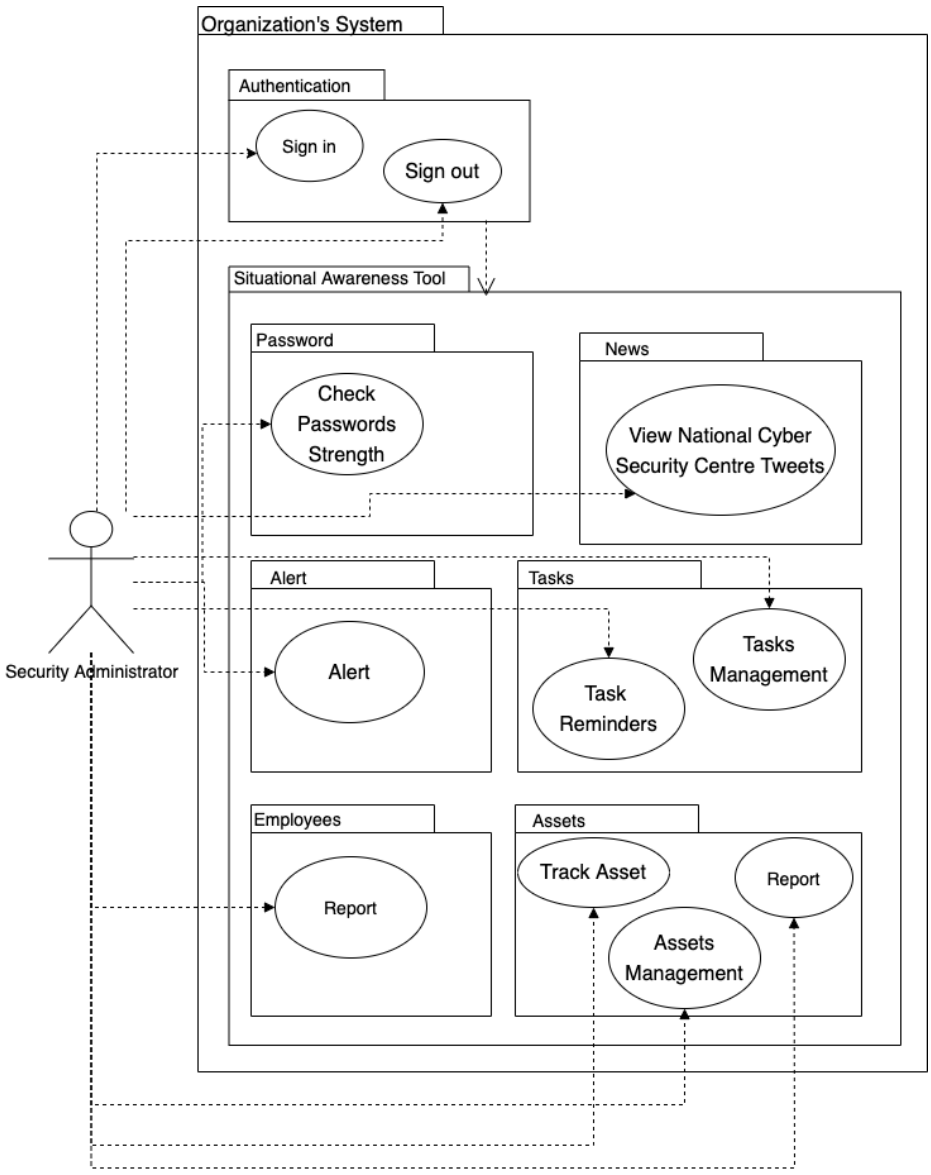

Figure 3: Use Case Diagram

4.3.1.3 Use Cases

Requirement 1: Check password strength

Preconditions:

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The security administrator opens the tool dashboard.

Main success scenario

Security administrator	Situational awareness tool
1. The security administrator requests that the tool is opened.	
	2. The tool checks the passwords according to the requirements.
	3. The tool calculates the percentage from Step 2.
	4. The tool displays the visualised results based on the percentage from Step 3 to illustrate the situation.

Post-conditions:

- The percentage indicating the extent to which the employees' passwords satisfy the password requirements represents in a pie chart. A detailed description of the passwords requirements is provided in Section 4.4.2.
- The passwords' strengths and weaknesses are displayed in many range charts.
- The charts are presented using colour coding. A detailed description of the color coding is provided in Section 4.4.3.
- The security administrator will be aware of the current situation.

The rest of use cases are included in Appendix A.

4.3.2 Non-functional requirements

In addition to the functional requirements, there are a number of important characteristics representing the non-functional requirements and these are as follows:

Table 4: Non-functional requirements of our tool

Availability	The tool must be available to use when the security administrator needs it.
Usability	The tool must be easy to use and learn.
Performance	The tool must interact with the security administrator in an acceptable response time.
Error handling	The tool must handle error situations and display the appropriate error message.
Multiple screen size	The tool must be compatible with multiple screen sizes.
Security	The tool must be secure and save the data because it is integrated with the organisation's system and has access to sensitive information.
Visibility	The tool must represent and visualise the information based on colour coding. Information regarding the use of colour coding is presented in Section 4.4.3.

4.4 Design

This section discusses the initial graphical user interfaces of the proposed tool as well as the standard for checking the passwords and the tool colour coding.

4.4.1 Initial graphical user interfaces (GUI) design

This section presents the initial GUI of the proposed tool. Because the aim is to implement requirement 1 (check password strength), the focus is on discussing this requirement as well as presenting the initial GUI. Meanwhile, the rest of the initial GUI are included in Appendix B. In order to check the strength of the employees' passwords, the results appear depending on certain requirements, a detail of these requirements is provided in Section 4.4.2. In addition, the results appear based on colour-coding to make the security administrator aware if there is something wrong, a detail of color-coding is provided in Section 4.4.3.

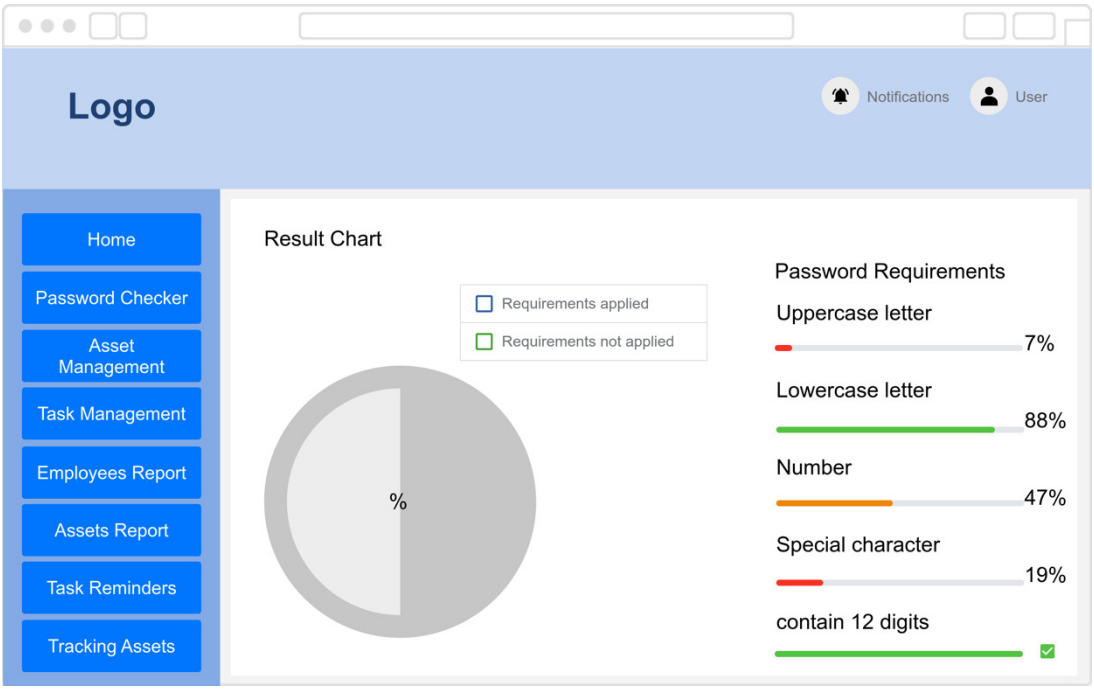

Figure 4: The initial design of requirement 1 (check password strength) page.

4.4.2 Password requirements

A strong password contains one uppercase letter, one lowercase letter, one number, and one special character and its length is 12 digits. Thus, the algorithm for the tool is designed based on this perspective with measures determining whether or not the passwords have satisfied requirements.

4.4.3 Situational awareness colour coding

The tool is designed based on the colour coding to give the security administrator a specific message regarding the current situation. The tool is based on three colour categories: red, amber and green.

- Red refers to:
  - Abnormal and unsecure situations that need to be alerted.
  - A device is far away from the organisation's boundary.
- Amber refers to:
  - Situations requiring attention because they present a moderate risk.
  - A device is close to the organisation's boundary.

- Green refers to:
    - Normal and secure situations.
    - The devices are within the organisation's boundary.

In addition, the tool relies on two colour categories which are grey and green in the pie chart that is displayed on the page for requirement 1 (check password strength):

- Grey refers to the requirements that have not been applied.
- Green refers to the requirements that have been applied.

Note: the colour coding is set based on the writer's knowledge.

4.5 Implementation

Due to the limited time allocated for this study, it focuses on implementing only requirement 1: check password strength. In addition, in the real-world, it is assumed that the proposed tool collects the organisation's data in order to function and arrive at a result but the current study relies on a dataset to test the tool. This section displays the GUI of the tool after the implementation and discusses the pseudocode of the password requirements. In addition, it explains the steps involved in performing the experiment at the end.

4.5.1 Implementation of requirement 1 (check password strength)

This section displays the graphical user interface of the implemented requirement (before it is run). Figure 5 below shows that there are some features that have not been discussed in the initial design which concern the selecting of the dataset and the record numbers. The selecting of the dataset makes it possible to choose a specific dataset and its records appear in the records number section (after running the tool) to make the user aware of its records number. In addition, there is a feature that will appear after running the tool which makes the user aware of the amount time it takes for the tool to process the dataset. This was designed in a blue font to make it clear. It was implemented for the purpose of the results and evaluation, thus it is not essential that they appear in the real-world design, a detail of the result and evaluation is provided on 5.3.

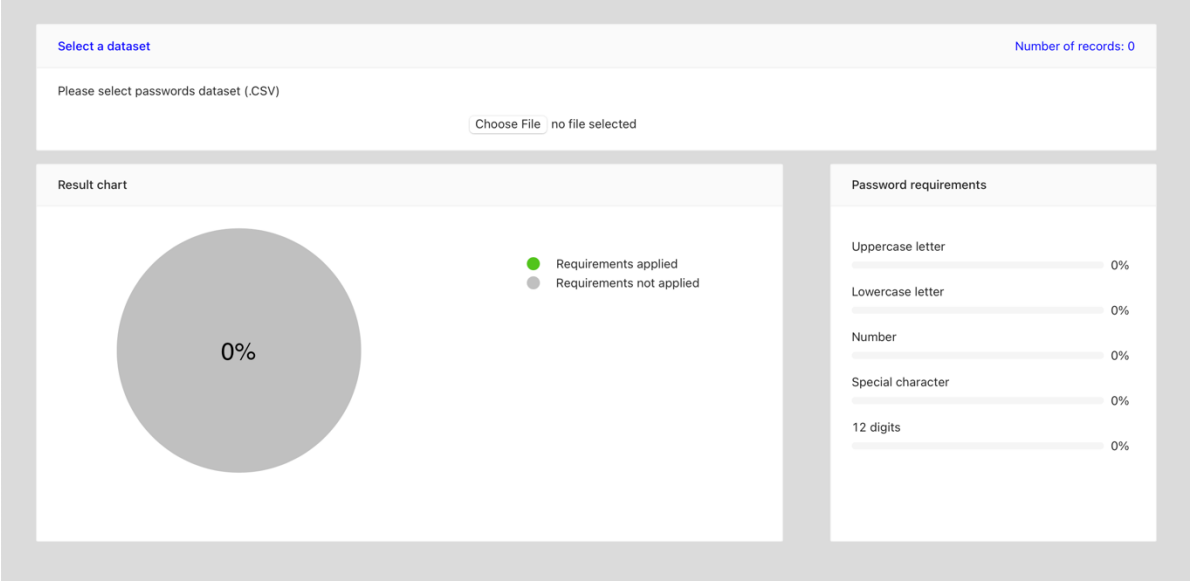

Figure 5: The final design of requirement 1 (check password strength) page.

4.5.2 Pseudocode of requirement 1 (check password strength)

This section discusses three pseudocodes. The main pseudocode is used to check password strength. The other two pseudocodes are for the functions needed in the main pseudocode which relate to calculating the percentage and colour.

Check password strength pseudocode

Description: The algorithm is used to measure the passwords' compliance regarding whether they contain one uppercase letter, one lowercase letter, one number and one special character, as well as being 12 characters in length.

Input: Password document (dataset)

Output: Return the percentages for use in visualising the results in charts according to the colour coding

```
Start
Get password document
Read password document
CountPasswordRecords ← Records Length
CountStrongPassword ← 0

CountUppercase ← 0
CountLowercase ← 0
```

```
CountSpecialCharacter ← 0
CountNumber ← 0
CountDigits ← 0

FOR each password in the document
      Points ← 0

      IF includeUppercase
            Points ++
            CountUppercase ++
      ENDIF

      IF includeLowercase
            Points ++
            CountLowercase ++
      ENDIF

      IF includeSpecialCharacter
            Points ++
            CountSpecialCharacter ++
      ENDIF

      IF includeNumber
            Points ++
            CountNumber ++
      ENDIF

      IF Password Length ==12
            Points ++
            CountDigits ++
      ENDIF

      IF Points == 5
            CountStrongPassword ++
      ENDIF
ENDFOR

CountNotStrongPassword ← CountPasswordRecords - CountStrongPassword

PercentageStrong ← Call function Percentage (CountStrongPassword,
CountPasswordRecords)
PercentageNotStrong ← Call function Percentage (CountNotStrongPassword,
CountPasswordRecords)
PercentageUppercase ← Call function Percentage (CountUppercase,
CountPasswordRecords)
PercentageLowercase ← Call function Percentage (CountLowercase,
CountPasswordRecords)
```

```
PercentageSpecialCharacter ← Call function Percentage
(CountSpecialCharacter, CountPasswordRecords)
PercentageNumber ← Call function Percentage (CountNumber,
CountPasswordRecords)
PercentageDigits ← Call function Percentage (CountDigits,
CountPasswordRecords)

ColorUppercase ← Call function Color (PercentageUppercase)
ColorLowercase ← Call function Color (PercentageLowercase)
ColorSpecialCharacter ← Call function Color (PercentageSpecialCharacter)
ColorNumber ← Call function Color (PercentageNumber)
ColorDigits ← Call function Color (PercentageDigits)

Return PercentageStrong, PercentageNotStrong, PercentageUppercase,
PercentageLowercase, PercentageSpecialCharacter, PercentageNumber,
PercentageDigits, ColorUppercase, ColorLowercase, ColorSpecialCharacter,
ColorNumber, ColorDigits
End
```

Calculate percentage pseudocode

Description: The algorithm returns the percentage result.

Input: Partial value, total value

Output: Return percentage

```
Start
Percentage  ← (100 * partial value) / total value
Return Percentage
End
```

Colour pseudocode

Description: The algorithm returns the colour result.

Input: Percentage

Output: Return the colour

```
Start
IF value <= 33
      Red
ELSE IF value <= 66
      Amber
ELSE IF value <= 100
      Green
ENDIF
Return Color
End
```

4.6 The experiment

The experiment was initiated by selecting and loading the dataset. The dataset was in a comma-separated value (CSV) format. Then the tool took time to read and process the uploaded data and details of the processing are given in Section 4.5.2. Subsequently, the results appeared on the screen. Clarification of the visualised results is discussed on the next chapter.

4.7 Environment setup

Requirement 1 (check password strength) in the proposed tool was implemented using react which is a JavaScript framework with an Ant design library for designing a graphical user interface (GUI). NPM and Node.js were used to download the project packages and to host the tool locally. Meanwhile, the Sublime Text tool was used for coding. The laptop utilised for the purpose of implementation was a MacBook Pro laptop running macOS Big Sur version 11.6 with 16 GB 2667 MHz DDR4 for the memory and 2.3 GHz- 8- Core Intel Core i9 for the processor.

4.8 Dataset description

The experimental datasets for this project were 000webhost, hak5, izmy, and Lizard-Squad (Miessler 2021) which were obtained from one of the GitHub accounts. The account has a set of many datasets such as usernames, passwords, sensitive data patterns, URLs, web shells, fuzzing payloads, and more. The owner of the account has mentioned that these datasets have been used throughout security assessments. The datasets were publicly available and they were in a readable format (CSV) and the Table 5 below displays the number of records.

Table 5: Datasets details

Dataset name	Records number
000webhost	720302
hak5	2351
izmy	1476
Lizard-Squad	11781

4.9 Summary

The proposed SA tool is assumed to run integrated with the organisation's systems to reflect the existing situation and raise awareness that could help mitigate data breaches in future. This chapter has discussed the functional and non-functional requirements of the proposed tool and described its initial design. In addition, the implementation of one function of its requirements (the MoSCoW methodology) is used due to the limited time allocated to complete the current study. The implemented function is requirement 1 (check password strength) and a password dataset has been applied to test the tool. The result of running the implemented function is presented in the next chapter.

Chapter 5: Results and Evaluation

5.1 Overview

After knowing the reasons that lead to the data breach issue, developing our SA tool and selecting the necessary datasets that were explained in the previous chapters, the tool was run for various datasets. In this chapter, we recommend a list of needed security requirements to help organizations be secure. Then we discuss how could existing solutions and our proposed SA tool aid in preventing data breaches. In addition, we discuss the results and evaluation of running our SA tool.

5.2 Result

The results of the current study are presented in this section. The first part lists the security requirements, whilst the second part discusses the experiments that have been conducted as well as the results obtained when the data were entered.

5.2.1 Security requirements

Based on our knowledge of the reasons behind data breaches and their existing solutions, we set a list of security requirements that the organisation needs to apply to minimise the possibility of experiencing breaches in future. Initially, we identified all entities associated with any organisation that the attackers could exploit at any stage of a data breach. The entities included the organisation's boundary and internal network, security administrator, employees, devices, servers and third parties. Then we set a total of 44 requirements for these entities (see Table 6: The security requirements that businesses must satisfy in order to be secure, as well as the role that existing security technologies play in meeting these needs. Moreover, it shows how the proposed tool could help enterprises meet). Whilst applying these security requirements could

significantly minimise the possibility of experiencing a breach, we do not want to suggest that these requirements are exhaustive. Indeed, some of the security requirements listed in Table 6 will be very difficult for many organisations to meet, especially if they are small or medium sized organisations because certain technical solutions are costly. Nonetheless, we believe that applying SA tools such our proposed tool or even other ideas with a similar concept would achieve good results at the lowest possible cost.

Table 6: The needed security requirements for businesses to be secure

	Existing non-technical solution		Existing technical solution								New Trend
	Training and raise awareness	Security policies	Firewall	Intrusion detection system	Intrusion prevention system	Data leakage prevention system	Anti-malware	Multi-factor authenticators	Encryption	Reliance on a third party	Our situational awareness tool
Security requirements for organisations to improve their security against data breaches											
Organisation boundary and internal network											
Detect phishing emails.				◑							
Block phishing emails.					◑						
Detect access of malicious websites.			◑	◑							
Block access of malicious websites.			◑		◑						
Prevent unauthorised physical access.		◑									
Encrypt sensitive data while transferring.									◑		
Analyse network traffic.				◑							
Configure security tools correctly such as Firewall, IDS, IPS, etc.	◑										
Employees											
Limit the number of attempts when signing in.		◑									
Apply multi-factor authentication when signing in.		◑						◑			
Use strong passwords.	◑	◑									◑
Deactivate their credentials when they leave the organisation.		◑									
Prevent access to sensitive data without admin permission.		◑									
No online information about the employee that could help attackers in their research.	◑										
Require passwords to be changed regularly.	◑	◑									◑

Prevent employees from uploading data or information to the internet.	◑	◑									
Do not allow sensitive information or data to be taken off the premises.	◑	◑									
Do not install files that could contain malware.	◑	◑		◑	◑		◑				
Security administrator (including all of the requirements for employees)											
Perform security risk assessments regularly.		◑				◑					◑
Perform penetration tests regularly.										◑	◑
Conduct security training for employees.	◑									◑	◑
Analyse the existing security policies regularly to suggest improvements.											◑
Manage access privileges of all employees effectively.			◑			◑		◑			
Apply multi-factor authentication when creating new users' accounts.		◑						◑			
Apply multi-factor authentication when changing any information relating to existing users' accounts.		◑						◑			
Update and patch the software when a vulnerability is disclosed.	◑										◑
Keep abreast of the latest information regarding cybersecurity.	◑										◑
Observe the level of the users' passwords in the organisation.											●
Devices											
Track the location of important devices.											●
Update and patch systems regularly.	◑										◑
Set strong passwords and change default devices' credentials.	◑	◑									
Change passwords whenever an employee with knowledge of them leaves the organisation.		◑									
Ensure files that could contain malware are not installed on devices.			◑	◑	◑		◑				
Servers											
Update and patch the server regularly.	◑										◑
Check the validity of the file types before uploading to the server.	◑	◑	◑								
Apply a strong network segmentation.		●	●								
Implement access control.		◑									
Encrypt all data, especially sensitive data.		◑							◑		
Third-party											
Prevent from accessing sensitive data.		◑									
Limit the number of attempts when signing in.		◑									
Apply multi-factor authentication when signing in.		◑						◑			
Use strong passwords.		◑									
Change passwords regularly.		◑									
Deactivate their credentials when a contract finishes.											◑

● The solution is fully effective
◑ The solution is partially effective

To summarise, Table 6 shows that the existing security countermeasures do not offer suitable detection and protection against targeted attacks that can lead to data breaches. This could be

due to various limitations associated with existing solutions including their inability to detect complex threats as well as zero-day assaults, high false alarm rates, and managerial reliance on human expertise. However, despite their limitations, these security solutions may still be effective for enterprises in terms of protecting against untargeted attacks perpetrated by cybercriminals and opportunists who do not use sophisticated strategies.

Organisations can use **firewalls, IDS, IPS, and anti-malware** to protect against known vulnerabilities and threats. However, a **firewall** cannot enforce a strong password policy or block the misuse of passwords. In addition, many means of obfuscation are used by hackers and high rates of false alarms adversely affect the performance of **IDS/IPS and anti-malware**. **DLPS** are effective against unwitting leakages that could be caused by employees when they upload sensitive data to the internet or export data off-premises but they are inadequate if attackers employ sophisticated techniques to hide their activities. **Multi-factor authentication systems** can make the task of hackers who depend on stolen credentials to access sensitive data more difficult, but they might adversely affect the system's usability and might increase the costs faced by the organisation in terms of replacing lost devices or the employee's time that would be lost during the authentication process. **Encryption** also increases the difficulty of understanding sensitive data in the event of a breach, thereby increasing the likelihood that the attackers would not benefit from the data. However, if the attackers were to discover the keys and decrypt the data, **encryption** would be considered insufficient. Finally, reliance on a **third party** to perform various tasks is very effective, particularly if organisations do not specialise in these tasks. For example, when performing penetration testing, organisations could rely on a **third party** but if the third party suffered from a breach, that would adversely affect the organisations it served and would not give a good result.

See Section 5.4 for a discussion of the tool that has been proposed.

5.2.2 The experiment results

This section displays the results of running the tool to process various datasets. The experiment is divided into four sections according to the different chosen datasets.

5.2.2.1 Experiment 1: 000webhost Dataset

Figure 6 presents the tool's GUI when run using the 000webhost data. It is apparent from the pie chart that the dataset's passwords fail to comply with the specifications stipulated in Section 4.4.2. For instance, only 21% of the passwords have 12 characters, 7% feature a special character and only 11% include an uppercase letter. However, the vast majority (98%) feature a number and a lowercase letter (97%). Colour coding is applied by the tool, with the entire pie chart being coloured grey to indicate that the passwords have failed to comply with the specified requirements. In terms of the individual requirements, in terms of including numbers and lowercase letters, both of these exceed 66% and are therefore coloured green. In contrast, the results for including 12 characters, a special character and uppercase letters are coloured red because none of these exceed 33%. See Section 4.4.3 for a discussion of the colour coding.

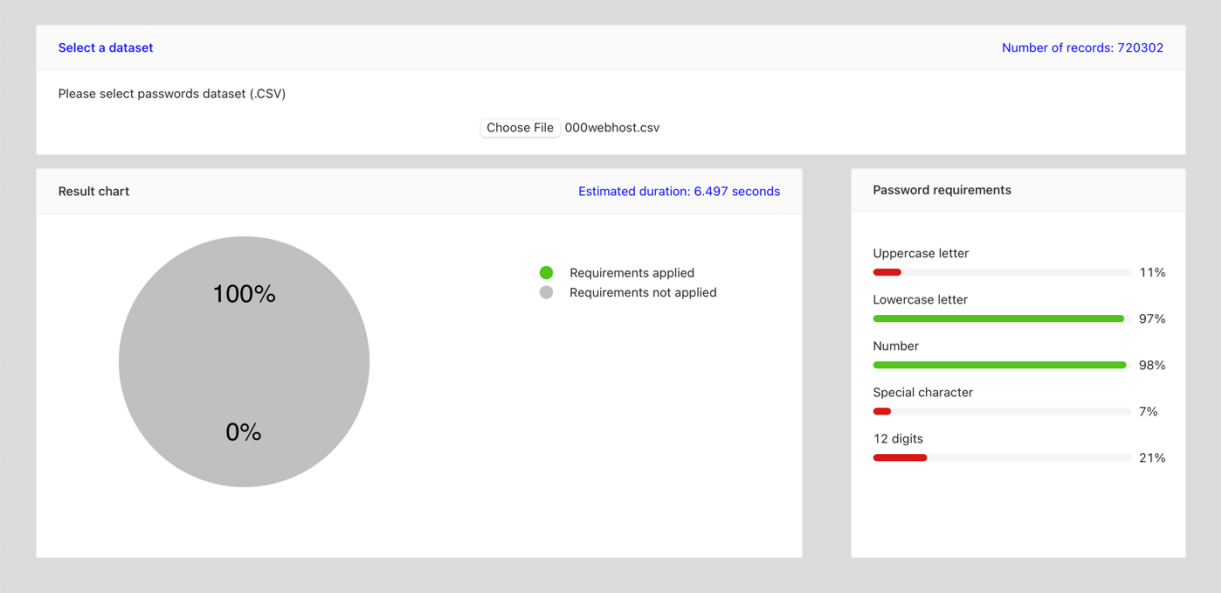

Figure 6: Result when choosing the 000webhost dataset

5.2.2.2 Experiment 2: hak5 Dataset

Figure 7 presents the tool's GUI when run using the hak5 data. It is apparent from the pie chart that only 2% of the passwords comply with the specifications stipulated in Section 4.4.2, whereas the remaining 98% do not. For instance, only 14% of passwords feature 12 characters, 8% include a special character, and 39% have an uppercase letter. However, most include a number (78%) and a lowercase letter (93%). Again, green is used to represent those passwords that comply with the stipulated requirements (including a number and using lowercase letters). Meanwhile, because the use of an uppercase letter falls between 33% and 67%, this is coloured amber. However, the remaining factors are coloured red to denote that their percentage results are below 33% (featuring 12 characters and including a special character).

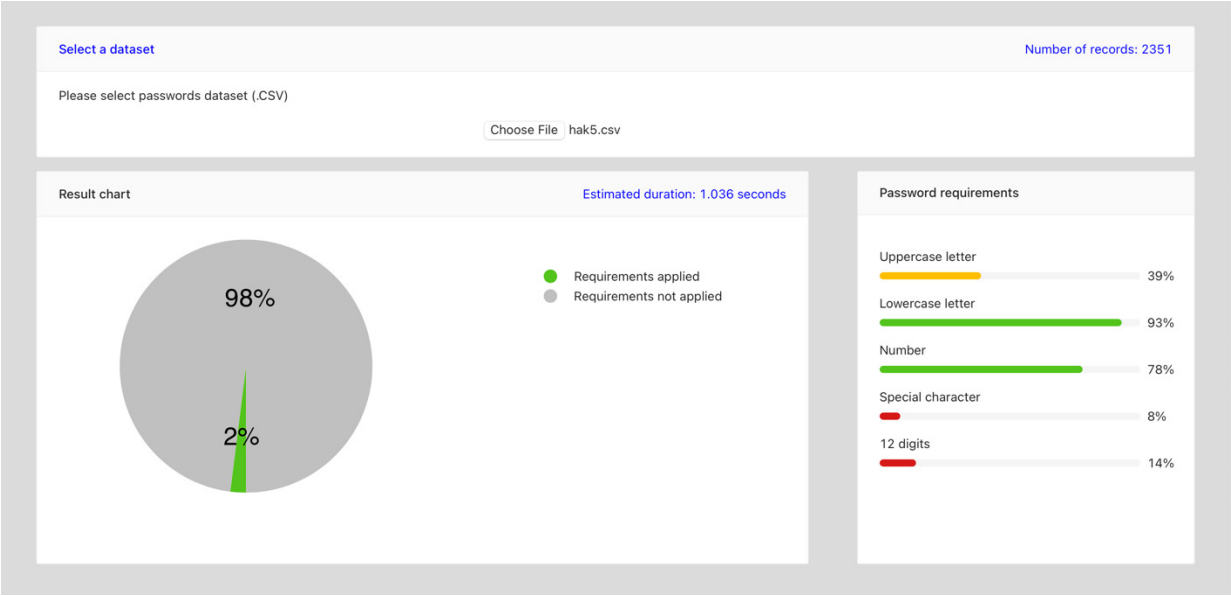

Figure 7: Result when choosing the hak5 dataset

5.2.2.3 Experiment 3: izmy Dataset

Figure 8 illustrates the tool's GUI when run using the izmy data. It can be seen that the pie chart indicates that just 2% of the passwords comply with the specifications stipulated in Section 4.4.2, whilst 98% of the passwords fail to comply. For instance, only 28% of the passwords feature a number, just 32% include an uppercase letter and 48% have a special character. In contrast, the vast majority include a lowercase letter (96%) and comprise 12 characters (97%). Therefore, the results for 12 characters and the inclusion of lowercase letters are depicted in green because

these exceed 66%. Meanwhile, the results for the use of a special character are coloured amber and those for featuring a number and an uppercase letter are coloured red, in accordance with the colour coding specified in Section 4.4.3.

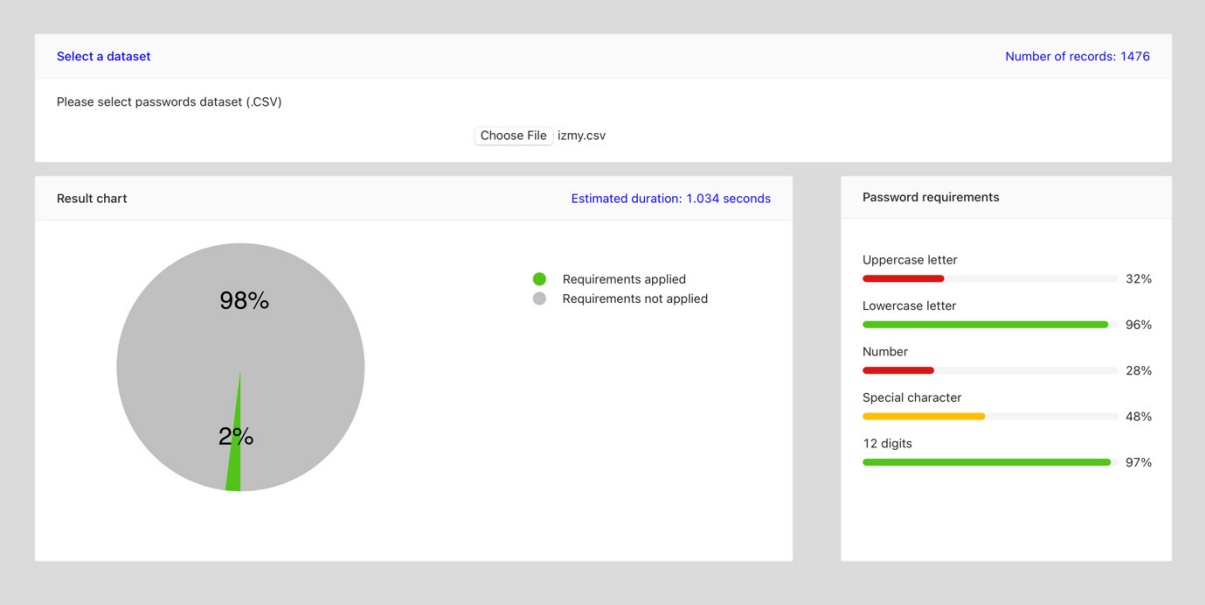

Figure 8: Result when choosing the izmy dataset

5.2.2.4 Experiment 4: Lizard-Squad Dataset

Figure 9 illustrates the tool's GUI when run using Lizard-Squad data. The pie chart shows that only 1% of the passwords comply with the specifications set out in Section 4.4.2, with the remainder failing to comply. For instance, just 7% of the passwords feature special characters, 16% include 12 characters and only 26% have an uppercase letter. However, the vast majority include a lowercase letter (94%) and a number (77%). In terms of colour coding, only the results for the inclusion of a number and a lowercase letter are depicted in green, whilst the other variables are coloured red.

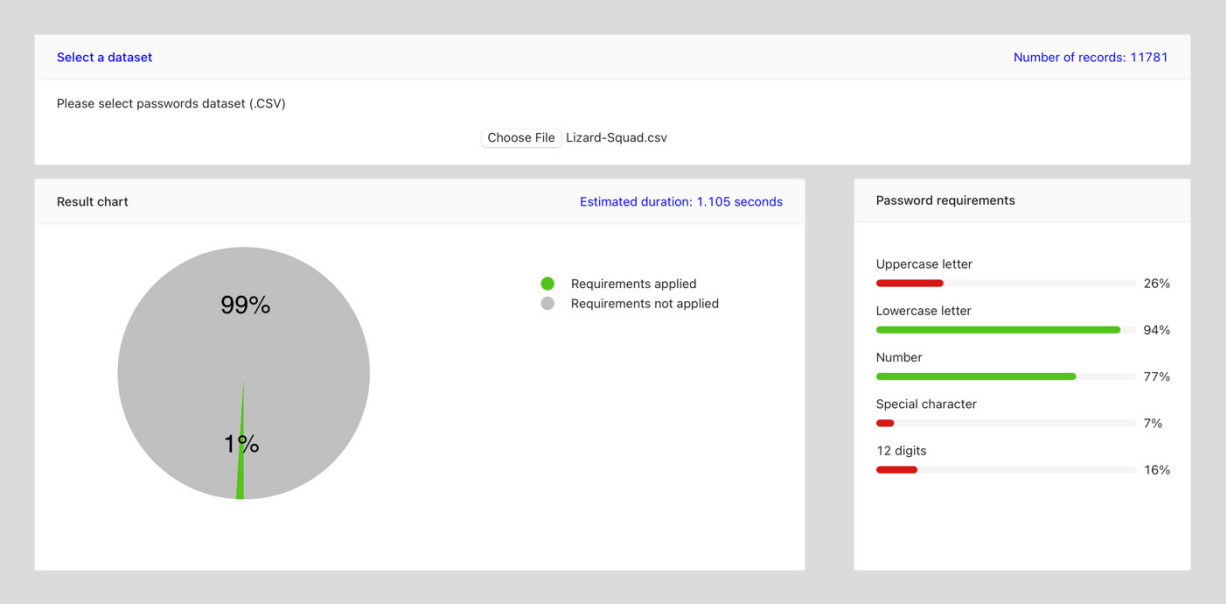

Figure 9: Result when choosing the Lizard-Squad dataset

5.3 Evaluation

The GUI results illustrated in Figures 6, 7, 8 and 9 establish the ability of the tool to depict the features of the passwords and present them on GUIs. As such, the selected tool makes a useful contribution in terms of improving situational awareness. It is also apparent that the tool has successfully colour coded the results in accordance with the approach specified in Section 4.4.3 to reflect the percentage outcomes.

The blue numbers that feature in the GUIs refer to the tool processing time and these confirm that there is a direct relationship between the number of password records in a dataset and the time taken to process the data. As such, an increase in the number of password records takes longer to process, thereby indicating that the tool is operating efficiently. Importantly, the time required to process the data is within the acceptable range in every experiment, thereby indicating that users are not left waiting for an extended period whilst the results are generated. The performance times and number of records in the dataset are presented in Table 7 below.

Table 7: Estimated processing time

Dataset name	Record number	Processing time (seconds)
000webhost	720302	6.497
hak5	2351	1.036
izmy	1476	1.034
Lizard-Squad	11781	1.105

Turning to Table 6 above, the security administrators would take appropriate decisions based on their knowledge regarding situations that lead to breaches. Since by implementing our proposed situational awareness tool:

1) The security administrators will be aware of the employees' password levels and they can make appropriate decisions regarding changing the password policy to make them strong enough. In addition, the security administrators will be aware of whether employees have changed their passwords regularly and the exact time of that change.
2) The security administrators can use the tool in all situations that need to be alerted such as an alert for performing regular security risk assessments; performing regular penetration tests; conducting security training for employees; regularly analysing existing security policies; and updating software, systems and servers. In addition, the tool will remind the security administrators to change or block any credentials of third parties on the date that their contract expires.
3) The security administrators will be aware of the latest information regarding cybersecurity.
4) The security administrators will know the dates for updating each device and will have the ability to track devices to pinpoint their location.

From the discussion above, it is possible to conclude that visualising the situation makes users more aware of what happens around them. Furthermore, our experiment results also show that using colour coding makes users understand and categorise situations, then make appropriate decisions at the right time before any damage is done. Consequently, we can confirm that data breaches can be mitigated by improving situational awareness.

5.4 Summary

This chapter has concluded our knowledge of the reasons for data breaches by creating a list of 44 security requirements to reduce the possibility of experiencing a data breach and it has been explained how the SA tool could be employed. In addition, we have conducted four experiments to test our proposed tool in detail using four public datasets. Then we and evaluated the results, emphasising the need for our SA tool.

Chapter 6: Conclusion

The current study has provided insight into the reasons behind data breach incidents. Then we stated a list of the necessary security requirements that could serve as a reference for organisations to remain secure against attacks that might lead to data breaches. We do not claim that these requirements are exhaustive because this area will be forever active and evolving. From another perspective, we found that applying SA helps to reduce risk and achieve perfect results. Thus, we recommended a tool that improves cyber SA. Only one function of the tool was implemented due to the limited time allocated for this study and we used four public datasets to test this function in our tool. The methodology applied in the current study consisted of three main sections which are the approach of the dissertation, the approach to develop the tool, and the results and evaluation approach. In addition, the methodology to develop this tool consists of four main phases: the identification phase; design phase; construct or build phase; and evaluation phase. The main finding of the current study is that visualising situations to ensure individuals are aware of what is going on around them is the best practice to reduce the likelihood of being hacked which can lead to a breach. This is because such an approach helps people to take appropriate decisions at the right time before any damage is done.

6.1 Limitations and future work

The important thing for any SA tool is to be understandable. As such, the user should understand the situation and be able to take suitable action at the appropriate time. Thus, our proposed SA tool's interface was designed in the English language and utilised the UK colour coding to give the purpose of its implementation when applied in organisations based in the UK. Conversely, the tool will be of no use if users do not understand the English language or have another meaning for the colour coding. Due to the short amount of time allocated for the current study,

the above-mentioned concerns could be used as a starting point for future studies to address. We recommend the following in particular:

- Designing interfaces that support multiple languages so that users have the ability to change the tool settings so that they are appropriate for the setting they are operating in.
- Taking into account the connotations of colours and their meanings for each community.
- Completing the build phase and implementing all of the requirements of the tool because we only implemented one function.

Finally, we would emphasise that the password requirements mentioned in Section 4.4.2 were selected from our own perspective and knowledge. Thus, we recommend following the latest policies regarding password strength requirements because this area is changeable and will certainly continue to evolve in the future.

Reflection on Learning

I am always believing in “Education is the passport to the future, for tomorrow belongs to those who prepare for it today” and believe that never stop learning gives people the chance to be distinguished from others and be ready for any challenges in the future. Completing my master’s degree and its dissertation was one of my goals in this life. This was not done without the god support and my supervisor guidance, Dr Neetesh.

The dissertation was started from choosing the topic and that phase was scary me as I was not sure which topic should I chose. Then I decided to dive in the data knowledge and understand the risk that it faces from cybersecurity perspective. Data breach is one of data risk. Thus, I believed that this topic would allow me to broaden my current capabilities and knowledge in a field that I am interested in. After choosing the topic, the next phase was reading in-depth to understand the topic and its problem, to suggest a best solution from my perspective. Finding a gap that I could contribute in was the most challenging phase for me. It was not easy as I was imagining since it took couples weeks of reading the data breach literature. This taught me the value of reading academic research and how it could be applied to expand my knowledge while also highlighting areas where I can improve. The second challenging thing was managing my time to finish the task and submit my dissertation on time. This project was the first work that I did alone. It taught me time-management skills, how to prioritize my tasks and schedule them, when should I give myself breaks.

Although writing my dissertation was an individual task, it was the most rewarding portion of my studying life since it taught me a variety of lessons and gave me with scientific and practical skills that I am confident will aid me succeed in the future. At the end I would say that the experience was really beneficial and will enable me to either advance and expand my work or engage in new experiences in my future professional and academic lives.

References

Adlakha, R., Sharma, S., Rawat. A. and Sharma K. 2019. Cyber Security Goal's, Issue's, Categorization & Data Breaches. *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon).* Faridabad; India, 14-16 Feb. 2019. IEEE Xplore. doi: 10.1109/COMITCon.2019.8862245

Agile Business Consortium. 2021. 10 MOSCOW PRIORITISATION. Available at: https://www.agilebusiness.org/page/ProjectFramework_10_MoSCoWPrioritisation [Accessed: 19 September 2021].

Ahmad,a A., Maynarda, B. S., Desouzab, C. K., Kotsiasc. J., Whittyd, M., Baskervillee, L. R., 2021. How can organizations develop situation awareness for incident response: A case study of management practice. *Computers & security* Vol.101. doi: 10.1016/j.cose.2020.102122

Alsaleem, B. and Alshoshan, A. 2021. Multi-Factor Authentication to Systems Login. *2021 National Computing Colleges Conference (NCCC)*. Saudi Arabia: Taif, 27-28 March 2021. DOI: 10.1109/NCCC49330.2021.9428806

Atif, A., Sean, M., Kevin, D., James, K., Monica, W. and Richard B. 2021. How can organizations develop situation awareness for incident response: A case study of management practice?. *Elsevier Ltd*. Volume101. doi: 10.1016/j.cose.2020.102122

Bertino, E., Terzi, E., Kamra, A. and Vakali, A. 2005. Intrusion detection in RBAC-administered databases. *21st Annual Computer Security Applications Conference (ACSAC'05*). doi: 10.1109/CSAC.2005.33

Bonneau, J., Herley, C., van Oorschot PC, and Stajano, F. 2012.The quest to replace passwords: a framework for comparative evaluation of web authentication schemes. *In: Proceedings of the IEEE symposium on security and privacy*, SP 2012, 21–23 May 2012, San Francisco, California, USA; 2012. p. 553–67.

Calder, L., Bhandari, A., Mastoras, G., Day, K., Momtahan, K., Falconer, M., Weitzman, B., Sohmer, B., Cwinn, A., Hamstra, S., and Parush, A. 2018. Healthcare providers' perceptions of a situational awareness display for emergency department resuscitation: a simulation qualitative study. *International Journal for Quality in Health Care*, Volume 30, Issue 1. doi: 10.1093/intqhc/mzx159

Cheng, L., Liu, F. and Yao D. 2017. Enterprise data breach: causes, challenges, prevention, and future directions: Enterprise data breach. Wiley interdisciplinary reviews. *Data mining and knowledge discovery*. Volume 7 (5). doi: 10.1002/widm.1211

Collinsa, L., Giblin, M., Stoszkowski, J. and Inkster, A. 2020. A study of situational awareness in a small group of sea kayaking guides. *Journal of Adventure Education and Outdoor Learning*. p.1-17. doi: 10.1080/14729679.2020.1784765

Cyware. 2018. What is Cyber Situational Awareness?. Available at: https://cyware.com/educational-guides/cyber-situational-awareness/what-is-cyber-situational-awareness-2ef4 [Accessed: 15 August 2021].

diagrams.net. 2021. Security-first diagramming for teams. Available at: https://www.diagrams.net/ [Accessed: 17 October 2021].

Endsley, M. R. and Garland D. J. 2000. Situation Awareness Analysis and Measurement. *Mahwah, NJ: Lawrence Erlbaum Associates*.

Endsley, M. R. 1999. Situation awareness in aviation systems. *In D.J. Garland, J.A. Wise & V.D. Hopkin (Eds.), Hand-book of aviation human factors* (pp. 257–276).

ENISA. 2020. ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. Available at: https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 [Accessed: 30 July 2021].

ENISA. 2020. ENISA Threat Landscape 2020 - Data Breach. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach [Accessed: 30 July 2020].

Fang, Y., Guo, Y., Huang, C. and Liu, L. 2019. Analyzing and identifying data breaches in underground forums. *IEEE Access* 7, 48770–48777. doi: 10.1109

Fore, A. and Sculli, G. 2013. A concept analysis of situational awareness in nursing. *Journal of advanced nursing*. Vol.69 (12), p.2613-2621. doi: 10.1111/jan.12130

GAO. 2018. Actions taken by equifax and federal agencies in response to the 2017 breach. Available at: https://www.gao.gov/assets/700/694347.pdf [Accessed: 5 October 2021].

have i been pwned?. 2021. Pwned Passwords. Available at: https://haveibeenpwned.com/Passwords [Accessed: 17 October 2021].

Hart M., Manadhata P. and Johnson R. 2011. Text Classification for Data Loss Prevention. In: Fischer-Hübner S., Hopper N. (eds) Privacy Enhancing Technologies. *PETS 2011. Lecture Notes in Computer Science, vol 6794*. Springer, Berlin, Heidelberg. Available at: https://doi.org/10.1007/978-3-642-22263-4_2

Hart S, B. 2016. After the data breach: Managing the crisis and mitigating the impact. *Journal of Business Continuity & Emergency Planning*, 9(4), pp. 317-328(12)

Holm, E. and Mackenzie, G. 2014. The importance of mandatory data breach notification to identity crime. *2014 3rd International Conference on Cyber Security, Cyber Warfare and Digital Forensic*, CyberSec 2014, 6-11.

Imperva Team. 2021. Data Breach. Available at: https://www.imperva.com/learn/data-security/data-breach/ [Accessed: 23 August 2021].

Joseph, C. R., 2017. Data Breaches: Public Sector Perspectives. *IEEE. IT Professional*. Volume: 20, Issue: 4. doi: 10.1109/MITP.2017.265105441

Karunakaran, S., Thomas, K., Bursztein, E., and Comanescu, O. 2018. Data breaches: user comprehension, expectations, and concerns with handling exposed data. *In Proceedings of the Symposium on Usable Privacy and Security*. 12 June 2018. USENIX.

Keszthelyi, A. 2013. About Passwords. Acta Polytechnica Hungarica. Vol. 10, No. 6. Available at: https://www.researchgate.net/publication/293518235

Kokkonen, T. and Puuska, S. 2018. Blue Team Communication and Reporting for Enhancing Situational Awareness from White Team Perspective in Cyber Security Exercises. *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Springer, Cham. doi: https://doi.org/10.1007/978-3-030-01168-0_26

Liu, D., Liu, X., Ma, L., Chang, Y., Wang, R., Zhang, H., Yu, H. and Wang, W. 2020. Research on Leakage Prevention Technology of Sensitive Data based on Artificial Intelligence. *2020 IEEE 10th International Conference on Electronics Information and Emergency Communication (ICEIEC).* Beijing; China, 17-19 July 2020. IEEE. doi: 10.1109/ICEIEC49280.2020.9152286

Malu, C., Chetan, G., Song, W., Umeshwar, D. and Miguel, D. 2012. A platform for situational awareness in operational BI. Decision Support Systems. Vol.52 (4), p.869-883. doi: 10.1016/j.dss.2011.11.011

Matthews, T. 2012. Passwords are not enough. *Computer Fraud & Security*. Volume 2012, Issue 5, Pages 18-20. Available at: https://doi.org/10.1016/S1361-3723(12)70044-1

Mayer, P., Zou, Y., Schaub, F. and Aviv, A. 2021. "Now I'm a bit angry:" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them. *30th USENIX Security Symposium*. Vancouver, B.C., Canada, 11-13 Aug, 2021. USENIX.

Miessler, D., 2021. Leaked Password Databases. Available at: https://github.com/danielmiessler/SecLists/tree/master/Passwords/Leaked-Databases [Accessed: 17 October 2021].

Nagaria, B. and Hall, T. 2020. Reducing Software Developer Human Errors by Improving Situation Awareness. *IEEE Software*. Volume: 37, Issue: 6. doi: 10.1109/MS.2020.3014223. pp 32 - 37

Okolica, J., Mcdonald, T., Peterson, G., Mills, R. and Haas, M. 2009. Developing Systems for Cyber Situational Awareness. *Proceedings of the 2nd Cyberspace Research Workshop.* Shreveport: Louisiana, USA, 20 March 2009. Research Gate. Available: https://www.researchgate.net/publication/297715305_Developing_Systems_for_Cyber_Situational_Awareness

Papadimitriou, P. and Molina H. 2010. Data Leakage Detection. *IEEE Transactions on Know; ledge and Data Engineering*. Volume: 23, Issue: 1. doi: 10.1109/TKDE.2010.100

proto.io. 2021. Prototyping for all. Available at: https://proto.io/ [Accessed: 17 October 2021].

Raigoza, J. and Jituri, K. 2016, "Evaluating The Performance of Symmetric Encryption Algorithms," *2016 International Conference on Computational Science and Computational Intelligence (CSCI)*. Las Vegas: NV, 15-17 Dec. 2016. IEEE. DOI: 10.1109/CSCI.2016.0258

Rajah, P., Dastane, O., Bakon, K., and Johari Z. 2020. The Effect of Bad Password Habits on Personal Data Breach. *International Journal of Emerging Trends in Engineering Research,* Volume 8. No. 10. Available at SSRN: https://ssrn.com/abstract=3716898

Rastenis, J. et al. 2019. Credulity to phishing attacks: a real-world study of personnel with higher education. *2019 Open Conference of Electrical, Electronic and Information Sciences (eStream).* Vilnius; Lithuania, 25 April, 2019. IEEE. DOI: 10.1109/eStream.2019.8732169

Raulerson, Evan L., 2013. Modelling Cyber Situational Awareness through Data Fusion. *MSc Thesis. Department of Electrical and Computer Engineering in Air Force Institute of Technology*. Available At: https://scholar.afit.edu/etd/898.

Rizzo P. R. 2018. Situational Awareness: A Leadership Phenomenon. Nursing science quarterly. Vol.31 (4), p.317-318. doi: 10.1177/0894318418792888

Robinson, K., 2021. Password Data. Available at: https://github.com/robinske/password-data [Accessed: 17 October 2021].

Roozbahani, F. and Azad, R. 2015. Security Solutions against Computer Networks Threats. *Int. J. Advanced Networking and Applications*. Volume: 7. Issue: 1. Pages: 2576-2581.

Saleem, A. and Naveed, M. 2020. SoK: Anatomy of Data Breaches. *Proceedings on Privacy Enhancing Technologies*. Vol.2020 (4), p.153-174. DOI: 10.2478/popets-2020-0067.

Sampaio, D. and Bernardino, J. 2017. Evaluation of Firewall Open Source Software. *13th International Conference on Web Information Systems and Technologies (WEBIST 2017)*. pages 356-362. DOI: 10.5220/0006361203560362

Satzinger and W. John. 2016. Approach to system development. *Systems analysis and design in a changing world.* Seventh edition. Australia : Cengage Learning.

Shapira, Y., Shapira B. and Shabtai A. 2013. Content-based data leakage detection using extended fingerprinting. *CoRR* abs/1302.2028.

Shu, X., Tian, K., Ciambrone, A. and Yao, D. 2017. Breaking the Target: An Analysis of Target Data Breach and Lessons Learned. *ArXiv e-prints*.

Spitzner, L. 2003. Honeypots: catching the insider threat. *19th Annual Computer Security Applications Conference, 2003. Proceedings*. Las Vegas, NV; USA. 8-12 Dec. 2003. IEEE. doi: 10.1109/CSAC.2003.1254322

Stewart, M. 2009. How to survive a data breach a pocket guide. United Kingdom: IT Governance Publishing

Tahboub, R. and Saleh, Y. 2014. Data Leakage/Loss Prevention Systems (DLP). *2014 World Congress on Computer Applications and Information Systems (WCCAIS)*. Tunisia: Hammamet. 17-19 Jan. 2014. DOI: 10.1109/WCCAIS.2014.6916624

Teymourloueiand, H. and Harris, V. 2018. Organization Risk Management on Network Vulnerability and Potential Data Breach. *2018 International Conference on Computational Science and Computational Intelligence (CSCI).* Las Vegas; USA, 12-14 Dec. 2018. IEEE. doi: 10.1109/CSCI46756.2018.00027

Trend Micro Team. 2021. Data Breach. Available at: https://www.trendmicro.com/vinfo/us/security/definition/data-breach [Accessed: 23 August 2021].

Zamosky, L. (2014). Avoid the breach: Put data security measures in place. Physician Executive, 40 (4), 82 – 84.

Appendix A

Requirement 2: Employees Report

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The tool provides a list of all functions that the security administrator can do.

Main success scenario

Security administrator	Situational Awareness Tool
1. The security administrator requests to see the employee report page.	
	2. The tool retrieves information about the employees.
	3. The tool displays table with all employee information
	4. The tool displays the security level of the passwords in color coding to visualize whether the password has been updated newly or from been a while.

Post-condition

- The table with all employee information displays.
- The updating date of their passwords and the security level displays according to color coding.
- The security administrator will be aware of the existing situation.

Requirement 3: Assets Report

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The tool provides a list of all functions that the security administrator can do.

Main success scenario

Security administrator	Situational Awareness Tool
1. The security administrator requests to see the assets report page.	
	2. The tool retrieves information about the assets.
	3. The tool displays table with all assets information.

Post-condition

- The table with all registered assets information displays.
- The security administrator will be aware of the existing situation.

Requirement 4: Track Asset

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The tool provides a list of all functions that the security administrator can do.
- All registered assets must have tracking SIM to connect and perform this function.

Main success scenario

Security administrator	Situational Awareness Tool
1. The security administrator requests to see tracking assets page or presses on the track button from assets report page.	
	2. The tool retrieves the tracking information of the connected devices on a map.

Post-condition

- The map appears with tracking information of all connected assets or of specific asset.
- The assets appear on map according to according to color coding.
- The security administrator will be aware of the existing situation.

Requirement 5: Alert

Precondition

- The availability of an internet connection to run the tool.

Main success scenario

Security administrator	Situational Awareness Tool
	1. The tool checks situations that need to alert: • The time for updating devices. • The time for performing the tasks • If any device took far away from the organization boundary.
	2. If the time is been for alerting or any asset has been located far away from the organization boundary.
	3. notification appears in the notification page.
	4. The notification sends to the security administrator email.
5. View notification on the tool dashboard and receive the email.	

Post-condition

- The notification appears on the notification page and sends to the security administrator email.
- The security administrator will be aware of the existing situation.

Requirement 6: Assets Management (Add - Update - Delete) Assets

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The tool provides a list of all functions that the security administrator can do.

Main success scenario

Security administrator	Situational Awareness Tool
1. The security administrator requests to see the assets management page.	
	2. The tool provides the security administrator a form to fill with asset information; model name, model number, software, last update date, reminder date, and tracking information.
3. The security administrator fills the form and submits it.	
	4. The tool checks the validates entered information.
	5. The tool informs the security administrator that the function is successfully completed.

Alternative scenario

A1: The security administrator requests to modify (update) asset information.

1. The A1 starts at point 1 of the main success scenario.
2. The tool displays a list of registered assets.
3. The security administrator selects the assets and update its information.
4. The scenario goes back to point 4.

A2: The security administrator requests to delete a device.

1. The A2 starts at point 1 of the main success scenario.
2. The tool displays a list of registered devices.
3. The security administrator selects the asset and deletes it.
4. The scenario goes back to point 5.

Exception scenario

E1: the security administrator left empty fields that are required.

1. The E1 sequence starts at point 4 of the main success scenario.
2. The tool informs the security administrator with a message Empty fields.
3. The scenario goes back to point 3 of the main success scenario.

E2: The security administrator adds a assets that already registered.

1. The E1 sequence starts at point 4 of the main success scenario.

2. The tool informs the administrator with a message that the asset is registered.
3. The scenario goes back to point 3.

Post-condition

- If the security administrator requests to add asset, the desired new asset will be added.
- If the security administrator requests to modify asset, the desired asset will be modified.
- If the security administrator requests to delete asset, the desired asset will be deleted.

Requirement 7: View National Cyber Security Centre Tweets

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The tool provides a list of all functions that the security administrator can do.

Main success scenario

Security administrator	Situational Awareness Tool
1. The security administrator enters the tool dashboard page.	
	2. The tool fetches tweets from chosen Twitter account to the dashboard.
	3. The tool displays the tweets.

Post-condition

- The tweets displays on tool home page and the security administrator does not need to visit Twitter and read them from the Twitter application.
- The security administrator will be aware of the existing situation.

Requirement 7: Task Reminders

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The tool provides a list of all functions that the security administrator can do.

Main success scenario

Security administrator	Situational Awareness Tool
1. The security administrator requests to see the task reminders page.	
	2. The tool retrieves information about the tasks.
	3. The tool displays table with all tasks.

Post-condition

- The table with all tasks detail displays.
- The security administrator will be aware of the existing situation.

Requirement 9: Assets Management (Update Asset)

Return to the alternative scenario section in requirement 6: assets management (add - update - delete) assets.

Requirement 10: Assets Management (Delete Asset)

Return to the alternative scenario section in requirement 6: assets management (add - update - delete) assets.

Requirement 11: Tasks Management (Add - Update - Delete) Task

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is authenticated.
- The tool provides a list of all functions that the security administrator can do.

Main success scenario

Security administrator	Situational Awareness Tool
1. The security administrator requests to see the task management page.	
	2. The tool provides the security administrator a form to fill with task information; task name, task detail, and task reminded date.
3. The security administrator fills the form and submits it.	

	4. The tool checks the validates entered information.
	5. The tool informs the security administrator that the function is successfully completed.

Alternative scenario

A1: The security administrator requests to modify (update) task information.

1. The A1 starts at point 1 of the main success scenario.
2. The tool displays a list of registered tasks.
3. The security administrator selects the task and update its information.
4. The scenario goes back to point 4.

A2: The security administrator requests to delete a task.

1. The A2 starts at point 1 of the main success scenario.
2. The tool displays a list of registered tasks.
3. The security administrator selects the task and deletes it.
4. The scenario goes back to point 5.

Exception scenario

E1: the security administrator left empty fields that are required.

1. The E1 sequence starts at point 4 of the main success scenario.
2. The tool informs the security administrator with a message Empty fields.
3. The scenario goes back to point 3 of the main success scenario.

Post-condition

- If the security administrator requests to add task, the desired new task will be added.
- If the security administrator requests to modify task, the desired task will be modified.
- If the security administrator requests to delete task, the desired task will be deleted.

Requirement 12: Tasks Management (Update Task)

Return to the alternative scenario section in requirement 11: tasks management (add - update - delete) task.

Requirement 13: Tasks Management (Delete Task)

Return to the alternative scenario section in requirement 11: tasks management (add - update - delete) task.

Requirement 14: Sign in

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is not authenticated in the tool.
- The security administrator must has password and username.

Main success scenario

Security administrator	Organization's System
	1. The organization's system displays the form of sign in.
2. The security administrator fill form.	
	3. The system validates what the security administrator filled.
	4. The system shows the list of functions related to the authenticated user and one of them will be the tool.
5. The security administrator presses on the tool button (Situational Awareness Tool).	
	6. The dashboard of the tool displays.

Exception scenario

E1: the security administrator enters a wrong password or username.

1. The E1 sequence starts at point 3 of the main success scenario.
2. If the authentication fails and the system informs the security administrator with a message Invalid password or username
3. The scenario goes back to point 1.

Post-condition

- If the authentication succeeds, the security administrator can use all the functions provided as well as use the tool functions.

- If the authentication fails, the system informs the security administrator with a message Invalid password or username.

Requirement 15: Sign out

Precondition

- The availability of an internet connection to run the tool.
- The security administrator is not authenticated in the tool.

Main success scenario

Security administrator	Situational Awareness Tool
	1. The tool displays sign out button.
2. The security administrator presses on sign out button.	
	3. The tool displays the sign in form of the organization's system.

Post-condition

- The security administrator logs out from the tool.

Appendix B

Requirement 2: Employees Report

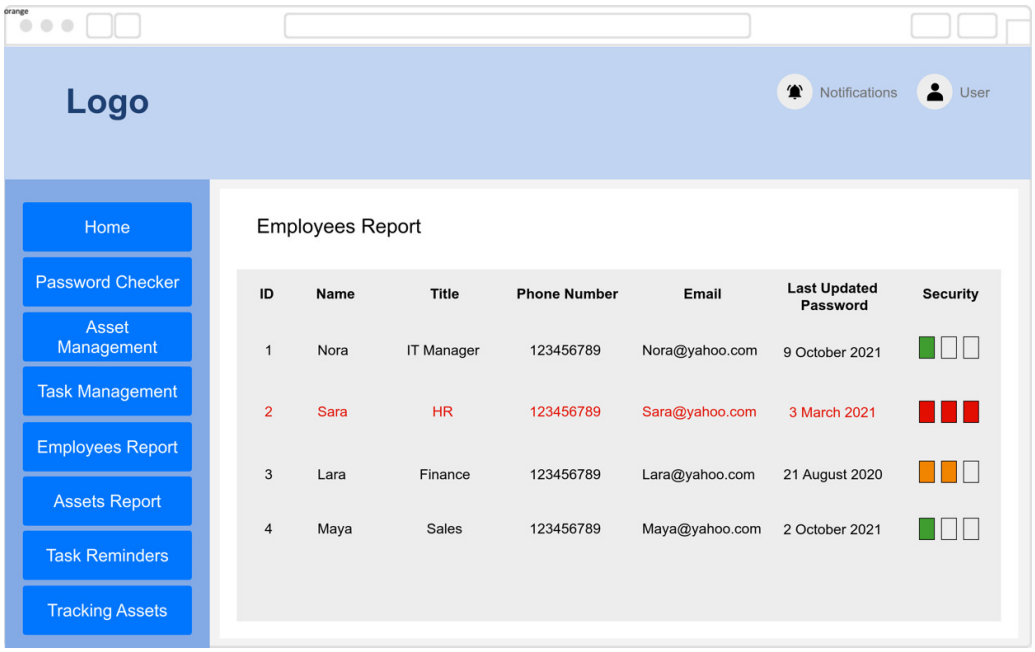

Figure 10: The initial design of requirement 2: employees report page

Requirement 3: Assets Report

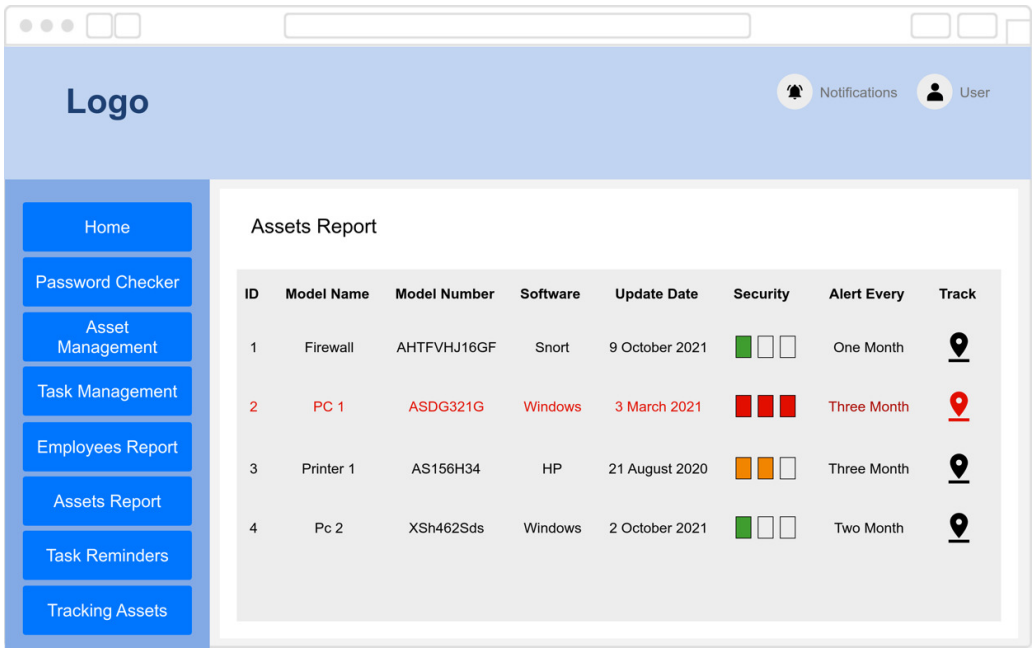

Figure 11: The initial design of requirement 3: assets report page

Requirement 4: Track Asset

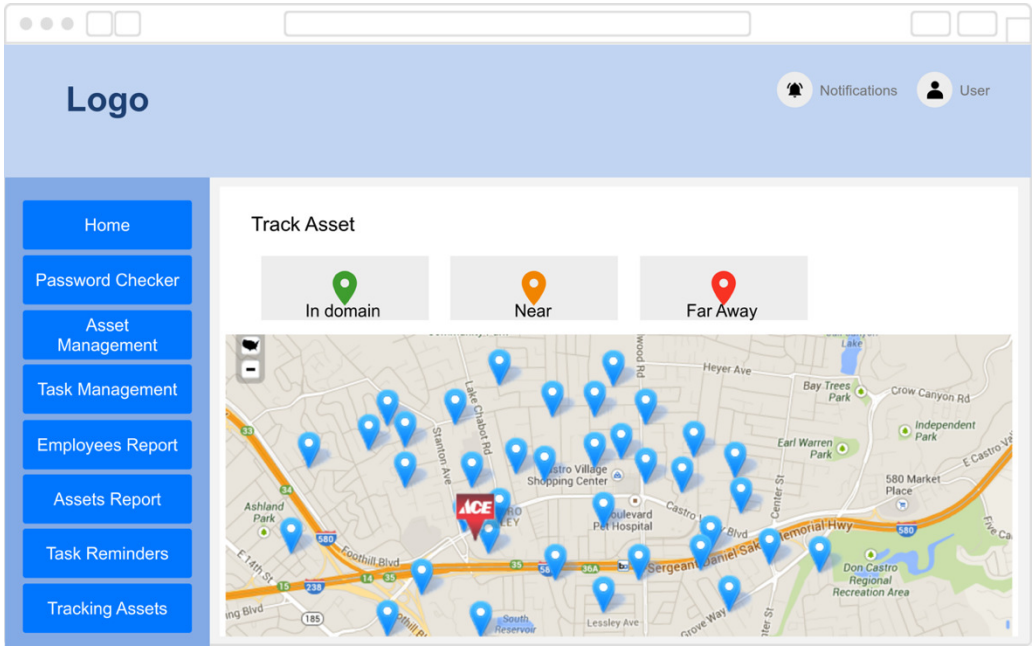

Figure 12: The initial design of requirement 4: track asset page

Requirement 6: Assets Management (Add - Update - Delete) Assets

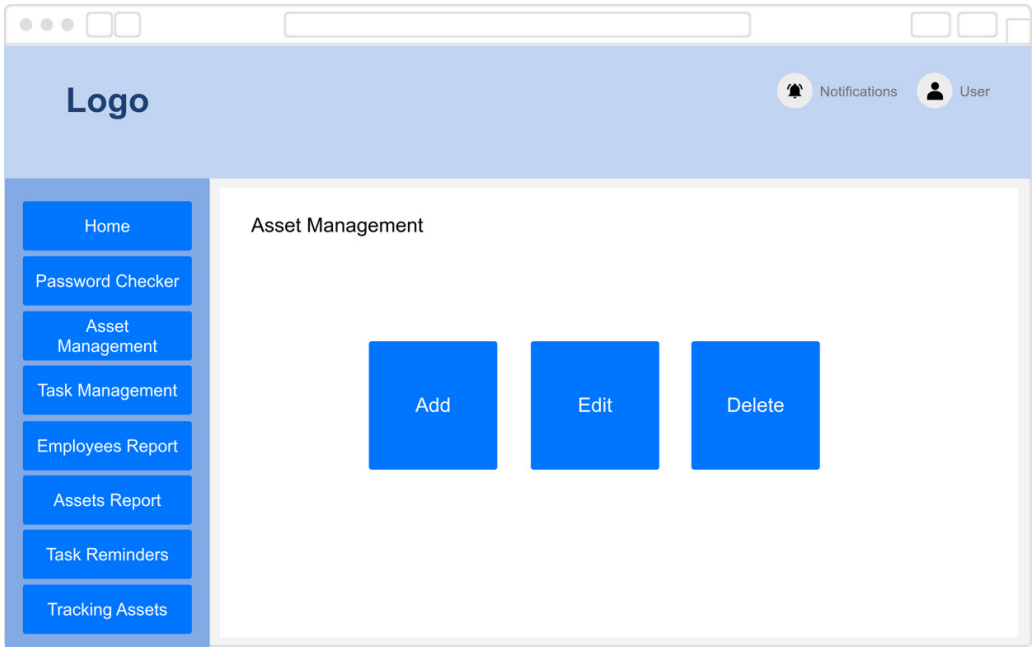

Figure 13: The initial design of requirement 6: assets management page

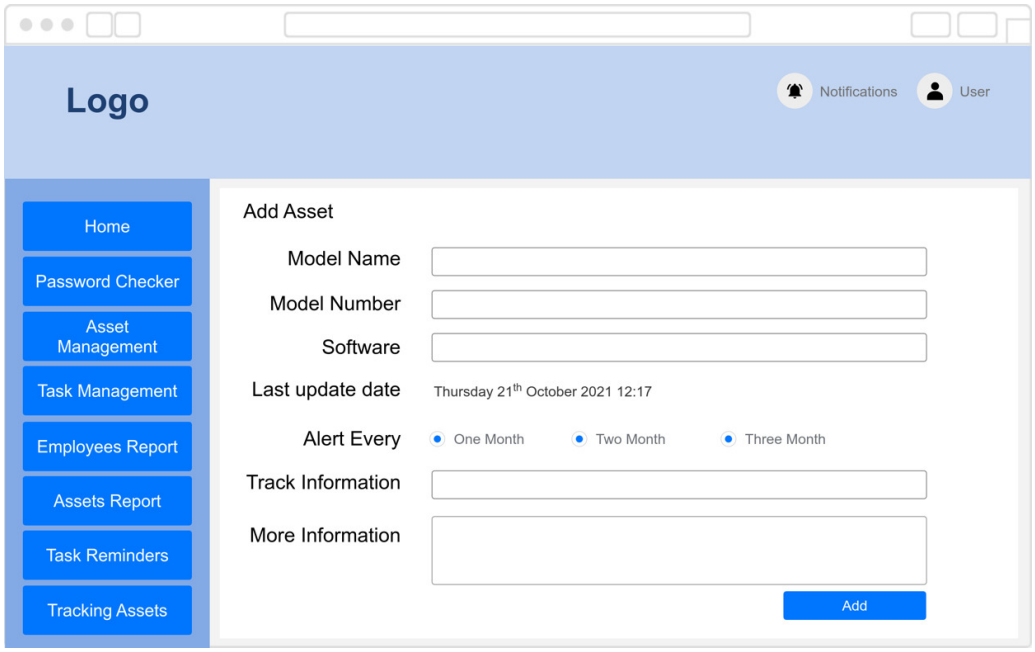

Figure 14: The initial design of requirement 6: assets management page (add)

Requirement 7: View National Cyber Security Centre Tweets

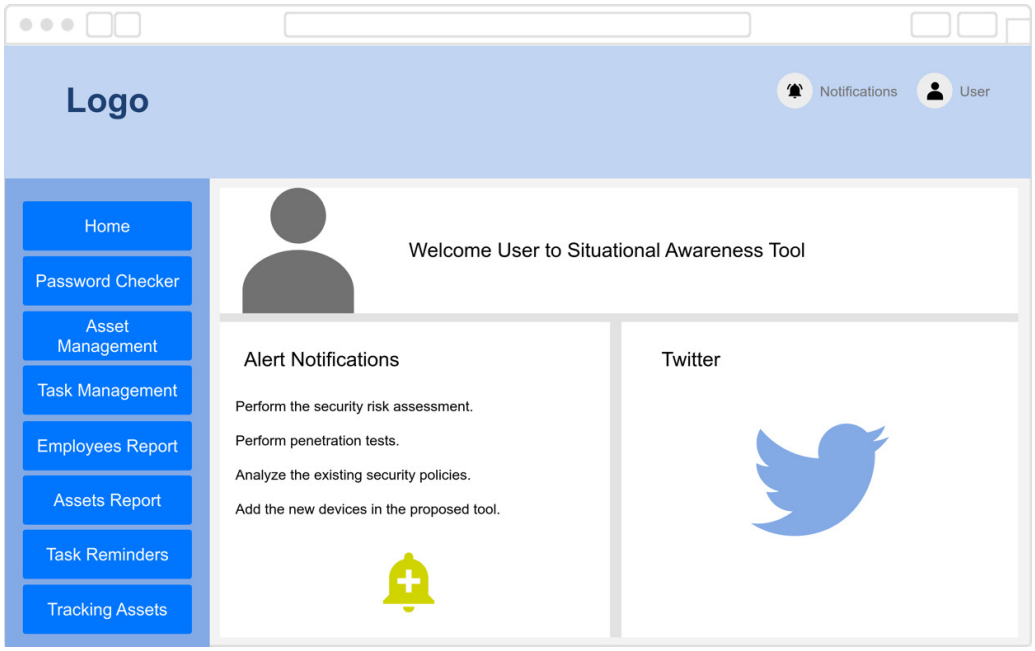

Figure 15: The initial design of requirement 7: View National Cyber Security Centre Tweets

Requirement 8: Task Reminders

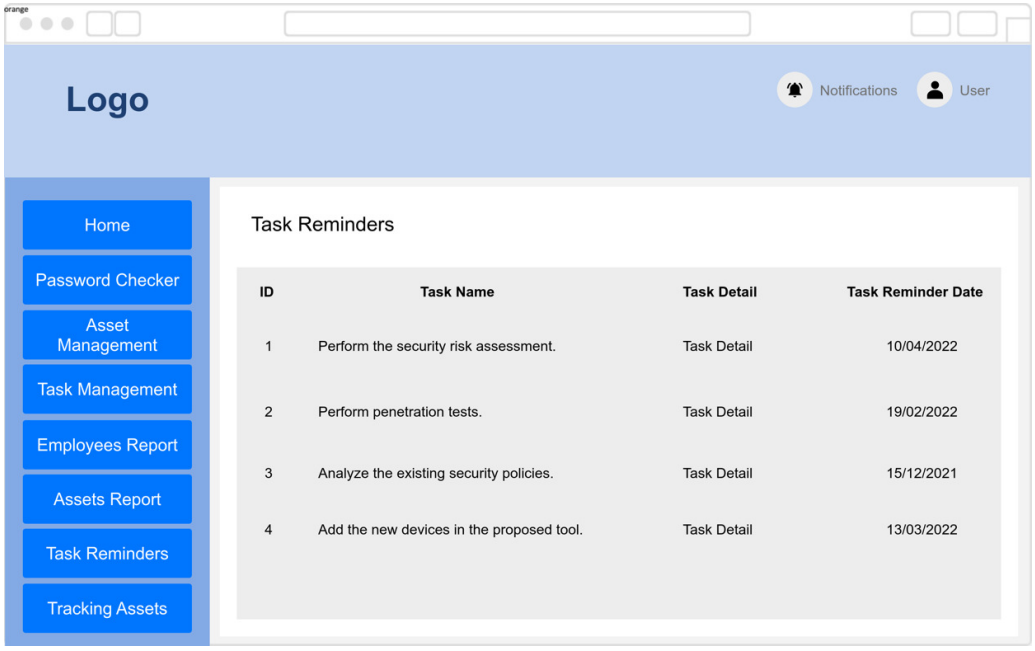

Figure 16: The initial design of requirement 8: task reminders page

Requirement 11: Tasks Management (Add - Update - Delete) Task

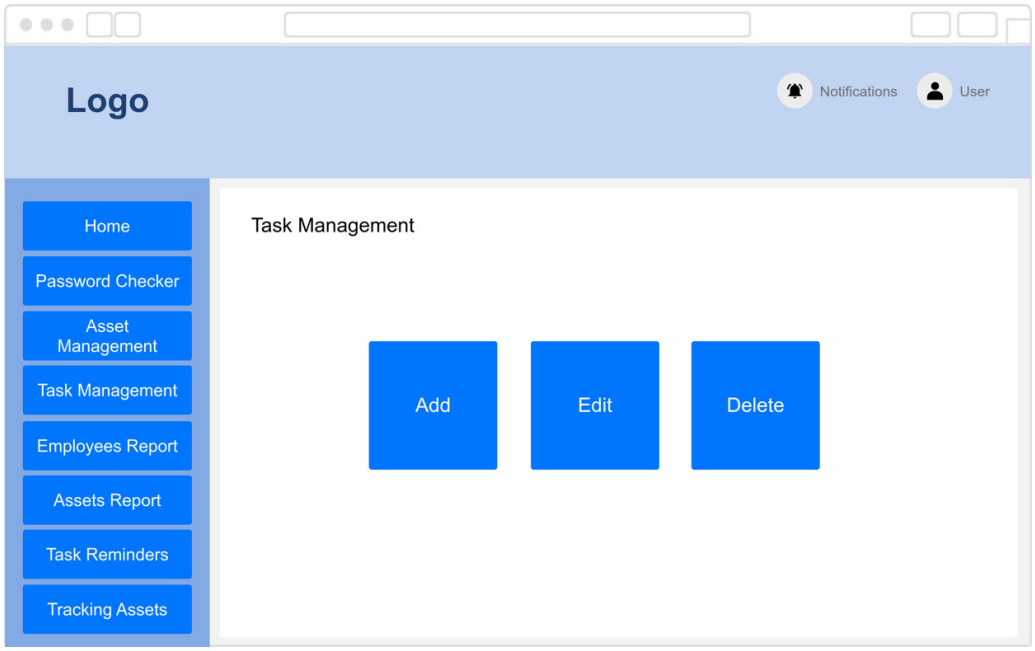

Figure 17: The initial design of requirement 11: tasks management page

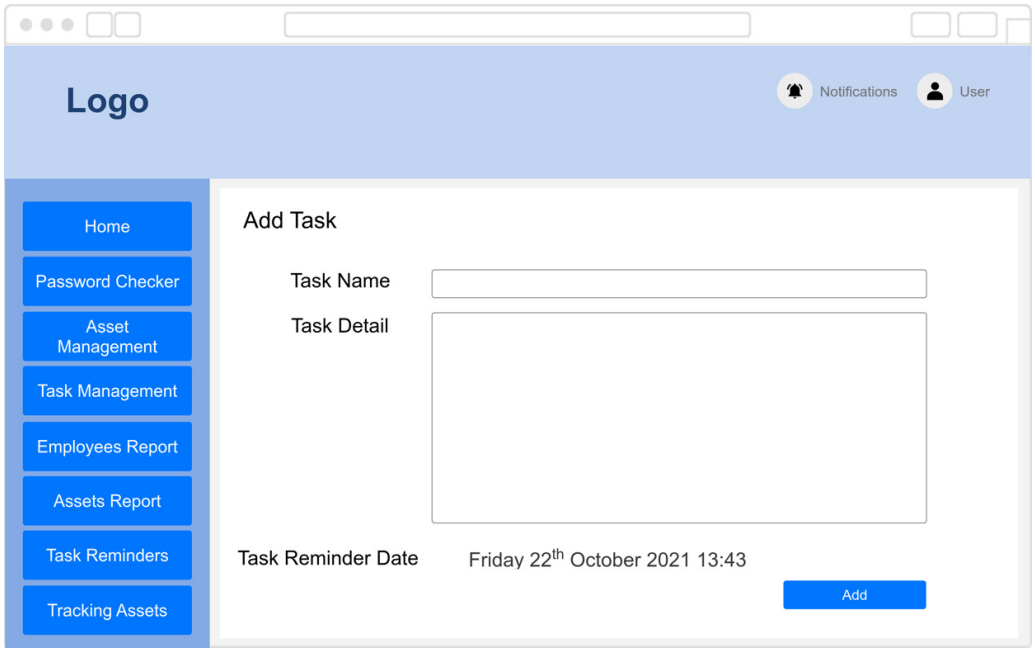

Figure 18: The initial design of requirement 11: tasks management (add)

Requirement 14: Sign in

After being the security administrator authenticated, the tool must appear on the organizations' systems homepage, thus the user would have the ability to authenticate the tool and use its functionalities.

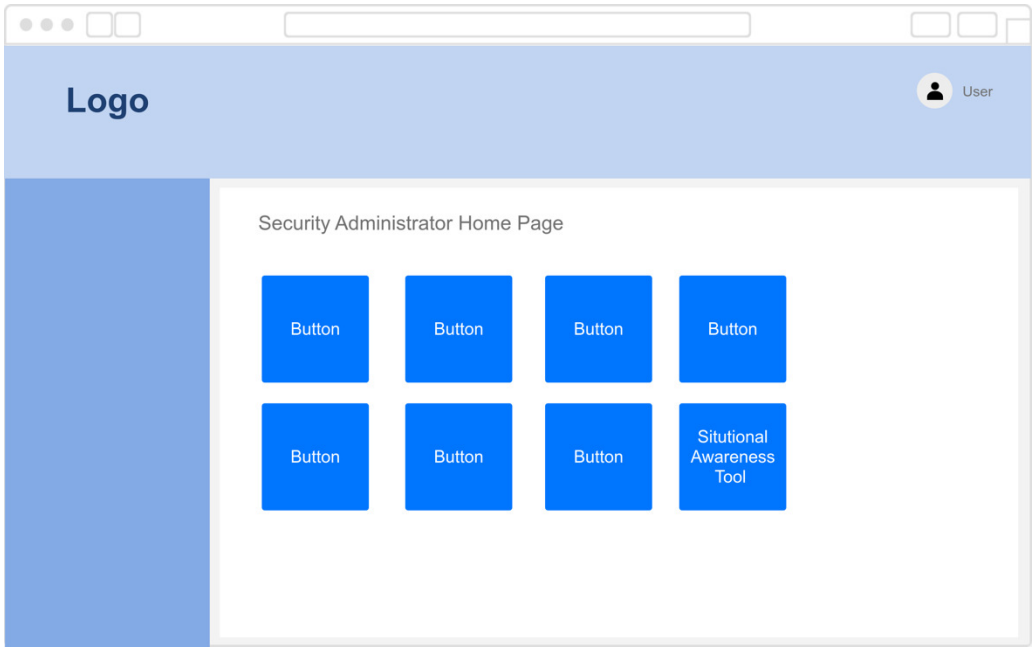

Figure 19: The initial design of appearing the tool on the organizations' homepage.