

**Establishing a Cyber Security Strategy and Hybrid Framework for Football Clubs in Scotland**

David Lawson

MSc Project Report – School of Computing

Matriculation Number: 1508178

Supervisor: Dr David Lonie

2024

Word Count: 12095

**Dissertation submitted in fulfilment of the requirements of the degree of Master of Science in Information Technology with Cyber Security, The Robert Gordon University**

**Declaration**

*“I affirm that this dissertation contains no unacknowledged copying of words or ideas from any publications or from any work written by another student or any other person. I affirm that any raw data collected during this research dissertation has not been falsified or duplicated and is available for inspection if required.”*

# Acknowledgements

I would firstly like to thank Dr David Lonie for his continued support and guidance throughout the formation of this project. His support over the last few months has been incredibly beneficial and vital to the development of this project.

Secondly, I would like to thank my friends and family for their support over the past year while I undertook this MSc degree – their words of encouragement, support, and laughter were key in motivating myself to finish my postgraduate degree.

Lastly, I would like to thank the Widening Access Department at Robert Gordon University, in particular Connor Anderson, Terri Foubister, Louise Durham, Anna Coats, and Sarah Eggleton, for their support, laughter, and motivation throughout the past year.

# Abstract

The movement into the digital era within sports organisations, particularly football clubs, has led to an ever-increasing reliance on digital infrastructure. This research project examines the potential threats surrounding cybersecurity that football clubs, particularly in Scotland, face, and proposes a new and unique hybrid cybersecurity framework to be used by said clubs in order to meet their specific needs. Through the use of qualitative research methods, this research project identifies the key vulnerabilities that these football club face and seeks to uncover the areas in which they can be exploited.

The hybrid cybersecurity framework is an amalgamation of the best areas of several different cybersecurity frameworks, established to understand and protect the unique nature in which football clubs operate. The framework is also designed to be adaptable and scalable, with football clubs of varying sizes being able to utilise it to ensure the highest degree of protection.

Through the use of case studies in the Scottish Football League system, the researcher clearly demonstrates the practical nature of the created hybrid cybersecurity framework; working closely with the case studies to analyse their cybersecurity strategies by undergoing a gap analysis and recommending improvements based on their results.

The implementation of a robust cybersecurity strategy is essential for football clubs to ensure operations can continue in a safe and protected manner in this modern, digital world.

# Table of Contents

Contents

[Acknowledgements 3](#_Toc174992457)

[Abstract 4](#_Toc174992458)

[Table of Contents 5](#_Toc174992459)

[Table of Figures 7](#_Toc174992460)

[Table of Tables 8](#_Toc174992461)

[1.0 Introduction 9](#_Toc174992462)

[1.1 Background 9](#_Toc174992463)

[1.2 Research Aim 10](#_Toc174992464)

[1.3 Research Objectives 10](#_Toc174992465)

[1.4 Research Questions 11](#_Toc174992466)

[2.0 Project Scope 12](#_Toc174992467)

[2.1 Introduction 12](#_Toc174992468)

[2.2 Literature Review 12](#_Toc174992469)

[2.3 Project Specification 13](#_Toc174992470)

[2.4 Overall Project Design and Implementation 13](#_Toc174992471)

[2.5 Findings 14](#_Toc174992472)

[2.6 Conclusions 14](#_Toc174992473)

[3.0 Literature Review 15](#_Toc174992474)

[3.1 Understandings of Security Threats 17](#_Toc174992475)

[3.2 Challenges Faced by Football Clubs When Implementing Security Strategies 20](#_Toc174992476)

[3.3 Risk Management 22](#_Toc174992477)

[3.4 Understandings of Cybersecurity Frameworks 23](#_Toc174992478)

[3.4.1 Securiti Qatar 2022 FIFA World Cup Cybersecurity Framework 23](#_Toc174992479)

[3.4.2 NIST Cybersecurity Framework 25](#_Toc174992480)

[3.4.3 CIS Control Framework 28](#_Toc174992481)

[3.4.4 NCSC Cyber Essentials Framework 29](#_Toc174992482)

[3.4.5 Analysis of Frameworks 31](#_Toc174992483)

[4.0 Project Specification 34](#_Toc174992484)

[4.1 Project Objective 34](#_Toc174992485)

[4.2 Project Methodology 35](#_Toc174992486)

[4.2.1 Project Research Design 35](#_Toc174992487)

[4.2.2 Project Data Collection 35](#_Toc174992488)

[4.2.3 Project Data Analysis 35](#_Toc174992489)

[4.3.4 Project Functional Requirements 36](#_Toc174992490)

[4.3 Issues Surrounding Legality, Ethics, Society and Professionalism 40](#_Toc174992491)

[4.3.1 Issues Surrounding Legality 41](#_Toc174992492)

[4.3.2 Issues Surrounding Ethics 42](#_Toc174992493)

[4.3.3 Issues Surrounding Society 42](#_Toc174992494)

[4.3.4 Issues Surrounding Professionalism 43](#_Toc174992495)

[4.4 Problems, Risks and Limitations 44](#_Toc174992496)

[5.0 Overall Project Design and Implementation 46](#_Toc174992497)

[5.1 Design of Hybrid Cybersecurity Framework 47](#_Toc174992498)

[5.2 Implementation 54](#_Toc174992499)

[5.3 Design of Practical Website 56](#_Toc174992500)

[6.0 Findings 61](#_Toc174992501)

[6.1 Overall Findings 61](#_Toc174992502)

[6.1.1 Findings of Case Study A 63](#_Toc174992503)

[6.1.2 Findings of Case Study B 64](#_Toc174992504)

[6.1.3 Findings of Case Study C 65](#_Toc174992505)

[6.1.4 Findings of Case Study D 66](#_Toc174992506)

[6.2 Summary of Findings 67](#_Toc174992507)

[7.0 Conclusions 69](#_Toc174992508)

[7.1 Case Study Evaluations 69](#_Toc174992509)

[7.2 Limitations 70](#_Toc174992510)

[7.3 Recommendations 71](#_Toc174992511)

[7.4 Recommendations for Future Work 72](#_Toc174992512)

[References 74](#_Toc174992513)

[Appendices 79](#_Toc174992514)

[Appendix A – Project Log 79](#_Toc174992515)

[Appendix B – Call for Case Studies & Further Discussions 81](#_Toc174992516)

[Appendix C – Gap Analysis 84](#_Toc174992517)

[Appendix D – Evaluation Documentation 86](#_Toc174992518)

[Appendix E – Website Test Cases 88](#_Toc174992519)

[Appendix F – GitHub Repository 90](#_Toc174992520)

# Table of Figures

Figure 3.1, PRISMA Methodology Flow Diagram……………………………………………………….………16

Figure 3.2, Securiti Qatar 2022 FIFA World Cup Cybersecurity Framework………………….……….24

Figure 4.1, Project Functional Requirements……………………………………………………….………….41

Figure 5.1, Split of Hybrid Cybersecurity Framework Categories…………………………….…………..53

Figure 5.2, Structure of Hybrid Cybersecurity Framework…………………………………….……………54

Figure 5.3, Website Flow Diagram………………………………………………………………………………….56

Figure 5.4, Website Index Page Wireframe………………………………………………………………………57

Figure 5.5, Database Design…………………………………………………………………………………………58

Figure 6.1, Case Study A Findings………………………………………………………………………………….63

Figure 6.2, Case Study B Findings………………………………………………………………………………….64

Figure 6.3, Case Study C Findings………………………………………………………………………………….65

Figure 6.4, Case Study D Findings………………………………………………………………………………….66

Figure 6.5, Summary of Findings……………………………………………………………………………………67

Figure B.1, Call for Case Studies……………………………………………………………………………………81

Figure B.2, Organisation of Meeting……………………………………………………………………………….82

Figure B.3, Summary of Meeting……………………………………………………………………………………83

Figure C.1, Gap Analysis………………………………………………………………………………………………85

Figure D.1, Evaluation Documentation…………………………………………………………………………..86

# Table of Tables

Table 3.1, NIST Cybersecurity Framework In-Depth Categories………………………………………….27

Table 3.2, Analysis of Cybersecurity Frameworks…………………………………………………………….33

Table 4.1, Project Functional Requirements……………………………………………………………………40

Table 5.1, Hybrid Cybersecurity Framework Design………………………………………………………….53

Table 6.1, Overall Findings……………………………………………………………………………………………62

Table B.1, Project Log………………………………………………………………………………………………….79

Table E.1, Website Test Cases………………………………………………………………………………………88

# 1.0 Introduction

## 1.1 Background

The sport of football has in recent years fully established itself in the digital age – technology underpins all aspects of the beautiful game, from employee and customer to information, to player statistics and key tactics: key areas of information that football clubs need to keep secure and confidential. As with any organisation, these football clubs are obliged to keep data secure and safe, but also face contextualised issues.

However, because of this venture into the digital age, football clubs have become prime targets for cybercriminals who are financially motivated to attack these organisations, seeking a large payday. Some of the world biggest football clubs have been targeted in recent years, notably Manchester United in 2020, who were attacked by a ransomware incident (Adler, 2020), and Paris Saint-Germain, whose ticketing services were hit by a cyberattack in April 2024, with the perpetrators potentially trying to size confidential customer information (Martin, 2024).

It is not just data that football clubs must keep secure and confidential. They must also consider the security of their physical assets: stadiums, training facilities, and offices must all be kept secure to ensure no unauthorised access is gained. One of the United Kingdom’s biggest clubs, West Ham United, had their stadium broken into in 2016 (Gaughan, 2016) – although no damage was done to the stadium or anything stolen, this shows that even the biggest clubs could face a devastating impact should others choose to steal or damage assets.

Football clubs are relying on technology to gain an upper hand against their competition, and to stay competitive in the fast-growing and ever-changing landscape of football: more matches, bigger tournaments, and wider audiences may seem like a significant benefit to the clubs, but in doing so, they significantly increase their risk of being attacked by cyber-criminals.

The motivation behind this project is to create a cybersecurity strategy and hybrid framework that football clubs can used to ensure the safety of their people, assets, and information. This piece of research aims to bridge the cybersecurity gap in relation to sports – no overarching framework dedicated solely to sports organisations exists, and so this piece of work seeks to address the gap for football clubs. This hybrid strategy will also be used to analyse and evaluate the already existing security strategies of several case studies who have agreed to participate in this research project.

## 1.2 Research Aim

The aim of this piece of research is to create a robust cybersecurity framework, developed by taking the best parts of already existing frameworks and formatting them together to create a hybrid model that will ensure the protection of a football clubs’ people, assets, and information, thus creating a secure digital and physical environment going forward.

## 1.3 Research Objectives

Several key research objectives have been identified and will be achieved throughout the formation of this research project. They are as follows:

* Development of an appropriate cybersecurity strategy to be used by football clubs within Scotland
* Formation of a hybrid cybersecurity framework, consisting of the best and most appropriate aspects of already-existing frameworks
* Analysis of already existing security strategies via case studies using the newly developed hybrid cybersecurity framework
* Provision of a comprehensive report that football clubs (and potentially other sports organisations) can use to improve their own cyber security strategies
* Creation of webpages to showcase the strategy and framework created throughout the development of this research project
* Creation of webpages to allow users to undertake their own risk assessment and gap analysis

## 1.4 Research Questions

From these research objectives, we can identify some key questions that must be addressed:

1. What security strategies are used by football clubs within Scotland and the United Kingdom?
2. What cybersecurity frameworks are readily available to be used by football clubs and businesses alike? What are their advantages and disadvantages?
3. What challenges and limitations stand in the way of football clubs implementing a robust cybersecurity strategy?

# 2.0 Project Scope

Here an overview of this research project will be provided, outlining and providing a small explanation of the different chapters used to create and develop the overall project at hand.

## 2.1 Introduction

This chapter seeks to provide the reader with an overall picture of the research project being developed, including the motivations behind the formation of the project, as well as the key research aims and objectives that the researcher is seeking to achieve while undertaking the research project.

## 2.2 Literature Review

This chapter seeks to provide the reader with an overview of already existing research surrounding and related to the chosen topic. Understandings of concepts such as cybersecurity, security strategies, and cybersecurity frameworks in relation to football and sports will be provided by the researcher. In doing so, the researcher will also identify gaps in the already existing research; gaps that the researcher seeks to fill throughout the formation of this research project. A literature review of merits and problems surrounding the implementation of cybersecurity frameworks will also be provided throughout.

## 2.3 Project Specification

This chapter seeks to provide a comprehensive outline of the steps that will be taken to achieve the research objectives that were outlined previously in this research project. Also in this chapter, the researcher will provide a detailed methodology, explaining how the research project will be developed, including key data collection and analysis methods. Consideration will also be given to issues surrounding legality, ethics, social issues and professional issues that may arise throughout the formation of this research project. Finally, consideration will also be given to analyse any problems or limitations that may arise during the research undertaken throughout the formation of this project.

## 2.4 Overall Project Design and Implementation

This chapter provides a comprehensive run-down, analysis, and justification of the chosen design of the hybrid cybersecurity strategy and framework. Analysing the advantages and disadvantages of several different already existing cybersecurity frameworks, and implementing them into this new hybrid model, while then applying said model to the existing security strategies of several different football clubs. The results from this implementation will act as a justification for football clubs around the United Kingdom to apply this new hybrid framework to their own security practices.

The results from this research project will also be showcased on an easy to navigate series of webpages, alongside a dynamic section, allowing for users to undergo their own gap analysis using the newly created hybrid security framework.

## 2.5 Findings

This chapter will seek to analyse the findings from the implementation of the hybrid cybersecurity framework previously discussed in this research project via a security gap analysis. Recommendations for security improvements will be made by the researcher, with intentions of bridging the gaps that may have arisen from the findings, and achieving the aims and objectives set out at the beginning of this piece of research.

## 2.6 Conclusions

Finally, conclusions will be drawn to summarise this research project. A summary of the key findings discovered because of this research will be drawn up, evaluating the positives and negatives that may have arisen throughout this research project. Conclusions will also be made based on the evaluation of feedback from football clubs that have been approached to take part in this research project – this feedback will involve to what extent the created hybrid framework was successful, and to what extent it was easily understood. Recommendations to improve security strategies will also be reiterated in this chapter, as well as discussions around any future research that may be undertaken that may stem from this research project.

# 3.0 Literature Review

This chapter seeks to investigate the literature that already exists surrounding the topic of security strategies and cybersecurity frameworks with relation to football and looking further into sports in general. The overall objective here is to identify the gaps in the literature that may lend themselves to be filled by the research project undertaken here.

To begin the analysis of already existing literature, a methodology of research had to be chosen. For this research project, *Preferred Reporting Items for Systematic Reviews and Meta-Analyses,* or *PRISMA*, for short, was chosen (Page et al., 2021; PRISMA, 2024), to search for the relevant research topic areas. The PRISMA methodology was initially applied to searches made via the RGU Online Library; however, the researcher soon discovered that using this online resource was limiting the scope of which existing research could be found, and so opted instead to use Google’s own academic database known as *Google Scholar* to search for the relevant research that already existed on the chosen topic area.

It is important to make note of what was searched to receive the results that was sought after. The following were key words and phrases used to gather sources and already existing research:

***(“Cybersecurity Framework” OR “Cyber Security Framework”) AND (“Football” OR “Soccer”) AND (“Cyber Defence” OR “Data Protection” OR “Cybersecurity Strategy”)***

The following flow diagram provides a visual and easy-to-understand display of the literature review undertaken by the researcher using the PRISMA methodology and the previous search query:

A flowchart of records

Description automatically generated

*Figure 3.1, PRISMA Methodology Flow Diagram*

Referring to the above *Figure 3.1*; to increase the levels of relevance, the search results were filtered to discard of anything written prior to 2014 – the researcher believed a 10-year scope would suffice for this research project. The researcher also ensured that research written out with of the English language should be excluded, as well as ensuring the exclusion of literature that were either opinion pieces, editorials, or non-peer reviewed journals. Duplicate pieces of literature were removed, and pieces of work with titles and abstracts not related to this research project were also excluded from the final number of studies included in the review.

## 3.1 Understandings of Security Threats

Football clubs are a business – they have employees and seek to make a profit. Although football clubs are very much entrenched in the digital age we now live in, they still face the same security threats that a ‘normal’ business would face; with some clubs facing massive amounts of risk, comparable to the biggest businesses we see in our everyday lives. Football clubs are increasingly relying on using technology to gain advantages and to make their operations more streamlined and expansive, and so must protect their information from unauthorised parties.

But what do we mean by protecting information? Samonas & Cross (2014) argue that the long-standing CIA Triad, meaning *Confidentiality, Integrity and Availability,* should be the benchmark for all information security practitioners to be following. It is important to understand what we mean when it comes to this triad: to begin with, *Confidentiality* entails the protection of information or data from any unauthorised party that may seek to access it. Next, *Integrity* entails the consistency and accuracy of said data, while also focusing on the completeness and overall reliability of the systems in which said data is stored. Finally, *Availability* entails the ability of authorised users to gain access to the systems and information stored on said systems, even when mitigating factors may be affecting the business (Kidd, 2023). Any threat to the data or information held by an organisation involves a breaching of either one, or a combination of, the CIA Triad – organisations and businesses must ensure that this does not take place to prevent detrimental actions taking place against them.

A breach of data can occur within any business, football club or not, and so no one business can ensure a perfect security strategy is in place. Breaching of any one of the CIA Triad will lead to a serious breach of data, and the longer it takes for the business to deal with it, the more catastrophic the damage to the business will be. According to Irwin (2022), from *IT Governance*, there are 5 main causes of data breaches within an organisation, they are as follows:

1. **Weak or Unlawful Use of Credentials**: The theft of user credentials is potentially one of the easiest ways to gain access to a private system. Many users rely far too heavily on easy to guess passwords, and many cyber criminals have access to modern pieces of software that can easily crack a user’s identity and gain unlawful access.
2. **Application Vulnerabilities**: Whenever a piece of software is released or updated, it may unknowingly be released with vulnerabilities. Cyber criminals can take advantage of these ‘back-doors’ and gain unlawful access to user systems – application developers must release patches for these vulnerabilities as soon as they are discovered to ensure damage is minimal. For example, social media platforms may be updated and now have what is known as *Broken Access Controls* – allowing attackers to access accounts and pages they should not be allowed to access (Chua, 2022).
3. **Malicious Software**: Perhaps the most well-known way in which access is gained to user systems, these pieces of software infect a user device or network through a vulnerability and usually impacts the user in a negative way. These can be simple pieces of software such as keyloggers, allowing attackers to steal key information from the user, or ransomware, where the attacker locks a system or holds information hostage in return for financial gain.
4. **Malicious Insiders**: Employees within an organisation have access to hundreds, potentially thousands, of confidential files; these employees may be attracted to undergo corporate espionage and send key information to a business’s competitors, or steal customer information, such as financial information, for themselves to either use or sell online.
5. **Insider Error**: Malicious activity is not the only way in which data can be breached, however. Simple employee error can lead to a breach of data. This can take the form of copying the wrong person into an email, attaching a private document to the wrong recipient, or even just losing a user device such as a laptop or a mobile phone.

Businesses, not just football clubs, must ensure their defences are up-to-date and fortified to the best of their abilities to ensure a cybersecurity incident does not take place and information is protected. Cyber-criminals need only one vulnerability to gain access to a user system or network, and so continuous cyber-audits must take place at regularly. Data breaches are not only costly on a financial level, but businesses and organisations also face professional costs – customers may simply not trust organisations should they face drastic cyberattacks and data breaches (Rawass, 2019; Sill, 2023).

## 3.2 Challenges Faced by Football Clubs When Implementing Security Strategies

Cybersecurity is often overlooked when it comes to a business’s everyday running, with many businesses either outsourcing their cybersecurity and IT support, or even having no security or support in place whatsoever. Football clubs are no strangers to this, and in fact, many football clubs simply do not recognise the need for cybersecurity, especially amongst clubs who are seen as smaller in comparison to the big names. Many of these clubs believe the work and information they do, and hold, are simply not worth the time for cybercriminals to try and go after – a wrongful assumption, as the data they do hold is simply too easy to gain access to (Manson & Pike, 2014).

During the 2022 FIFA World Cup in Qatar, emphasis was placed on the possibility of cybersecurity threats occurring. Because of the high levels of reliance on technology during the tournament, the Qatari government and FIFA had to work together to ensure the event, its participants, and its customers were appropriately protected. The likes of accommodations, ticketing systems, broadcasting systems, and transportation all relied on this digital infrastructure, and so multiple vectors of attack could be opened should cybercriminals gain access through vulnerabilities – this complex IT infrastructure was incredibly diverse and involved the integration of already-existing legacy infrastructure. With multiple platforms and devices used by employees, football clubs, and football fans, the hosts had to ensure this *Internet of Things* was protected to the best of their ability (Al-Dosari, et al., 2023; Seloom, 2024). This reliance and need for protection have been echoed by ordinary football clubs who have recognised that this is the world we now live in, with FC Barcelona dedicating and naming an official cybersecurity partner of the club, helping to secure the digital environment of the club, its assets, and its information (Thorpe, 2024). This expansion and integration of already existing infrastructure poses many challenges for football clubs when implementing security strategies.

Another massive challenge faced by football clubs who are keen on implementing a security strategy, is that of the financial aspect. Of course, the larger the football club, the more capital they have to ensure their assets are protected – but what of those clubs who ply their trade in a lower league, who cannot afford to have an ongoing, appropriate level of protection? Many of these lower league football clubs also do not have a dedicated IT team, with many either outsourcing their IT needs, or simply not taking advantage of any IT within their business. Because of this, many clubs face very high levels of risk when it comes to the breaching of data – many cybercriminals, with the appropriate knowledge, could easily take advantage and exploit the lack of protection that these football clubs simply cannot afford to implement. It is important to note that it is not just football clubs that run this risk, but ‘mainstream’ businesses in general that also could be exploited (Patterson, 2017).

Football clubs also face a challenge in the fact that they are high-profile targets – brands with a massive international following in all countries around the world. Many cybercriminals may see these high-profile targets and perpetrate cyber-attacks to gain high levels of media coverage – they may also hit these targets not just for financial gains, but also to serious damage the brands reputation, especially around football matches that are perceived as high-stake matches. Cybercriminals would keep a close eye on the security strategies that these clubs put in place to keep an open eye on any vulnerabilities that may arise, so that they may access their systems and drastically damage the club’s reputation (Grow & Shackelford, 2020).

These are but a few of the challenges that football clubs may face when it comes to the implementation or improvement of a cybersecurity strategy. It is important to summarise here that if a football club were to be hit by a cyberattack, then the cost on both a financial and reputational level would be catastrophic – it is generally accepted that it would cost football clubs a lot less in the long run if they were to be proactive in ensuring that cyberattacks are prevented from happening, rather than spending and losing a lot of money responding to, and finally overcoming from any cyberattacks that may be committed by cybercriminals (Pelzer, 2021).

## 3.3 Risk Management

Businesses and football clubs, small and large alike, are always at risk of cyberattacks, and so a system must be set in place to ensure threats are appropriately assessed, and measures are ready to be implemented should threats need addressed – the larger businesses and football clubs usually have some sort of system in place, but the smaller clubs usually need to be more attentive and ready to respond to threats as football clubs are cementing themselves in this digital age (Bada & Nurse, 2019).

But how do these football clubs implement these security systems to ensure the risk to their business and brand is managed? There are numerous, free-to-use, industry-standard cybersecurity frameworks readily available that can be used by football clubs, to ensure best practices are undertaken when formulating a security strategy and ensuring a good level of cybersecurity is up to the highest of standards. These frameworks ensure the protection of a business’s information, people, and its assets, and will significantly reduce the chances of a cyberattack being perpetrated by cybercriminals and other deviant external, or potentially even internal, parties (Crawley, 2021).

The following sub-chapter will seek to understand some of the frameworks that are already available for businesses and football clubs around the world to use and implement, completely free of charge.

## 3.4 Understandings of Cybersecurity Frameworks

As discussed; numerous free-to-use, industry standard cybersecurity frameworks are readily available to be utilised by the relevant parties when creating a cybersecurity strategy. These frameworks are utilised to create the strongest cybersecurity strategy possible, where protection from external, or even internal, parties is of the most importance. Different frameworks may support different categories of businesses in several different ways – there is no framework that is a *one size fits all* framework. Considerations need to be made with regards to funding, as well as availability of resources and personnel (Baker, 2021). The following sub-chapters will seek to discuss and analyse some cybersecurity frameworks that may be utilised to create a sound level of protection – this is by no means a comprehensive list, but only a small outlook into the possible options for businesses, and football clubs, alike.

### 3.4.1 Securiti Qatar 2022 FIFA World Cup Cybersecurity Framework

The first of its kind to be formulated purely for a footballing event, the Securiti (2024) framework developed for the Qatar 2022 FIFA World Cup was developed to ensure a smooth and safe running for the event, aimed at addressing data-related issues that comes with the World Cup. Created in 2018 but refined in 2022, this framework now acts as an industry standard for the biggest sporting events in the world (Malik, 2024).

This framework is designed with three fundamental pillars in mind:

1. **Prevention**: This pillar is concerned with preventing issues from occurring, and involves security relating to networks, endpoints and applications, as well as involving data protection. With regards to the data protection aspect, this ensures that data is held securely with regards to the data protection laws of that country – for example, this framework was developed with the Qatari Personal Data Privacy Protection law in mind (Securiti, 2023).
2. **Detection**: This pillar is concerned with the overall and on-going security monitoring and overall operations of the events and matches taking place.
3. **Response**: This pillar is concerned with how the relevant parties will respond to any situation that arises, including incident handling, as well as how they will recovery and continue operations to the highest standard.

A diagram of a security system

Description automatically generated

*Figure 3.2, Securiti Qatar 2022 FIFA World Cup Cybersecurity Framework*

A framework that is still in its infancy, it sets a good industry standard with events related to football, rather than event hosts or football clubs having to rely on other cybersecurity frameworks that may fail to cover all aspects of these niche businesses. Emphasising ‘must have’ aspects of cybersecurity principles, the framework is one that football clubs should consider when implementing a security strategy.

### 3.4.2 NIST Cybersecurity Framework

Perhaps one of the most well-known cybersecurity frameworks available to be used, the NIST, or *National Institute of Standards and Technology*, framework helps to reduce and manage cyber risks using a variety of high-level outcomes that are easy to understand, assess, prioritise and communicate to the relevant parties within an organisation (NIST, 2024).

Recently updated and developed with industry leaders within the workplace, academia and government, the framework focuses on 6 key areas with regards to dealing with any security strategies. As found in the NIST Handbook (2024), they are as follows:

1. **Govern**: This function dictates the establishment of an organisation or businesses cybersecurity risk management strategy, as well as how said organisation and businesses communicate and monitor the processes.
2. **Identify**: This function dictates how any potential cybersecurity threats are understood, as well as identifying the assets belonging the organisation. Finally, considerations are also given to any ways in which improvements to policies and procedures may be identified and implemented.
3. **Protect**: This function dictates what safeguards are put in place to ensure the organisations cybersecurity risks are mitigated to an acceptable level. Ensuring priority is given to risks that may be more detrimental to the organisation, steps such as training and implementing user authentication are taken, as well as ensuring the technological infrastructure of the organisation is up-to-date and protected.
4. **Detect**: This function dictates how any possible cyber risks are discovered, tracked, and analyse. Focusing on anomalies and any other indicators, this area of the framework also supports the response and recovery made by the organisation.
5. **Respond**: This function dictates which actions are taken by the organisation or the relevant parties following a breach in cybersecurity and a cyberattack taking place. This covers issues such as incident management, reporting, and risk analysis.
6. **Recover**: Finally, this function deals with how organisations and businesses respond to a cyberattack, and how best to get the organisation back running to their usual standard.

These 6 key areas are then further broken down into more in-depth categories. The following table, *Table 3.1,* provides a clear description of the categories covered by each of the functions detailed above:

|  |  |  |
| --- | --- | --- |
| **NIST Function** | **NIST Category** | **Category Identifier** |
| **Govern** | Organisation Context | GV.OC |
| Risk Management Strategy | GV.RM |
| Roles, Responsibilities, and Authorities | GV.RR |
| Policy | GV.PO |
| Oversight | GV.OV |
| Cybersecurity Supply Chain Risk Management | GV.SC |
| **Identify** | Asset Management | ID.AM |
| Risk Assessment | ID.RA |
| Improvement | ID.IM |
| **Protect** | Identity Management, Authentication, and Access Control | PR.AA |
| Awareness and Training | PR.AT |
| Data Security | PR.DS |
| Platform Security | PR.PS |
| Technology Infrastructure Resilience | PR.IR |
| **Detect** | Continuous Monitoring | DE.CM |
| Adverse Event Analysis | DE.AE |
| **Respond** | Incident Management | RS.MA |
| Incident Analysis | RS.AN |
| Incident Response Reporting and Communication | RS.CO |
| Incident Mitigation | RS.MI |
| **Recover** | Incident Recovery Plan Execution | RC.RP |
| Incident Recovery Communication | RC.CO |

*Table 3.1, NIST Cybersecurity Framework In-Depth Categories*

Very much an industry-standard framework used by organisations around the world, it does suffer from some drawbacks. Crawley (2021) argues that organisations who lack the capital or resources may not be able to implement the framework to a full extent, and so may risk leaving gaps in the security strategy they end up implementing. However, the framework does benefit from being easy to understand, and quick to implement should organisations choose to use and follow the framework that has been developed by NIST (Moschovitis, 2018).

### 3.4.3 CIS Control Framework

Another extremely popular framework used by organisations and business around the world, the CIS Control Framework is like the NIST Cybersecurity Framework detailed above, providing a security strategy that is easily understood by the common layman – many argue that this framework is the first stepping stone before using resources to implement the NIST framework on a full scale. This framework helps organisations to be critical about whatever existing strategy they have in place, with controls being split into 3 key categories:

1. **Basic**: This control involves the understanding of an organisation’s assets; anything that could have access to any key information or data that the business would like to keep confidential.
2. **Foundational**: This control circles around guidance that can be perceived to be a little more advanced – involving the implementation of technical aspects such as malware defence, account monitoring, and secure network configurations, to name but a few areas.
3. **Organisational**: Finally, this control is all about emphasising the know-how of relevant parties in an organisation when it comes to best cybersecurity practices. A strong cybersecurity program is worthless without employees knowing how to operate in the cyber-sphere safely – this control seeks to make use of security training, and the management of software life cycles. It also focuses on aspects such as incident responses, management procedures, and puts emphasis on penetration testing – ensuring that the cybersecurity strategy put in place is robust and can handle attacks (CIS, 2024).

These 3 categories can be further split into 20 sub-categories to ensure a robust security strategy is set in place. According to Carbide (2024), organisations who have implemented a security strategy following the CIS Control Framework, have seen a reduction in successful cyberattacks being perpetrated by as much as 85 percent. This framework allows for organisations to prevent attackers from exploiting their *‘poor cyber hygiene’,* such as out-of-date software and outdated solutions, and gives them peace-of-mind that their security strategy is held to a high industry standard.

### 3.4.4 NCSC Cyber Essentials Framework

Finally, we have the NCSC, or the *National Cyber Security Centre,* Essentials Framework – this framework is industry standard in the United Kingdom and beyond. Backed by the UK Government, it involves 5 key areas in in which organisations can implement security controls to protect from cyberattacks that may be perpetrated by cyber-criminals. Developed with costs in mind, it provides organisations with a low-cost option to cybersecurity, allowing for organisations to implement a security strategy, no matter the size or the resources available to them (NCSC, 2024).

The 5 key controls covered by the NCSC Cyber Essentials Framework are as follows:

1. **Firewalls and Routers:** Firstly, the framework provides key suggestions on how to improve the safety provided by firewalls and routers used by an organisation – recommendations surround creating a barrier to protect the network from any unauthorised attempts to access it.
2. **Software Updates**: Next, this framework provides recommendations surrounding software, ensuring that any software used by the organisation is up to date with the latest patches installed, helping to ensure any discovered exploits are covered.
3. **Malware Protection:** Working together with the Software Updates Control, this area covers recommendations surrounding anti-virus software and ensuring said software is updated and aware of the newest pieces of malware being used by cybercriminals.
4. **Access Control:** Next, this control deals with establishing a concrete definition of who should be able to access which pieces of information held by the business.
5. **Secure Configuration:** Finally, the framework provides recommendations on how to best ensure devices connected to the organisations network are best protected, and only those who need access to specific areas receive said access, helping to reduce exposures to cyberattacks. This area of control works together with the Access Controls recommended by the framework (IT Governance, 2024).

As previously stated, this framework is a low-cost option to cybersecurity. However, organisations can spend more money to receive NCSC Cyber Essentials Certification, named *Cyber Essentials Plus* – this allows for a licensed, technical expert to undertake and provide a security strategy for the organisation, rather than implementing framework recommendations by an in-house team. This allows for organisations to receive peace of mind that their business is not only secure from cyberattacks, but also adhering to legislation laid out by the government of the United Kingdom (UK Government, 2023).

### 3.4.5 Analysis of Frameworks

All the previous frameworks discussed throughout this chapter come with a variety of different benefits that would aid any organisation when creating a security strategy based on a chosen framework. It is important to identify where each framework thrives with regards to its advantages, but it is also equally as important to identify where each framework falls short. The small analysis undertaken in this chapter will help to create the hybrid cybersecurity framework that the researcher seeks to create as part of this research project, by taking the advantages of certain frameworks to help create a new overarching framework with the fewest number of demerits possible.

The following table, *Table 3.2,* provides an easy-to-understand analysis of the previously discussed cybersecurity frameworks:

|  |  |  |
| --- | --- | --- |
| **Framework** | **Advantages** | **Disadvantages** |
| **Securiti Qatar 2022 FIFA World Cup Cybersecurity Framework** | Industry specific – a good benchmark for those looking to create a strategy in the specific industry of football. | Potentially very costly to implement, using lots of resources due to the sheer size of the cover provided by the framework. |
| Holistic approach – covering multiple layers of security including cybersecurity, physical security and data protection. | Potential issues surrounding scalability – framework was originally designed for the biggest event in the world, and so may be difficult to implement on a smaller scale. |
| Lends itself to collaboration – framework was designed with multiple stakeholders, enhancing the level of security provided by the framework. | Potentially complex to implement the framework depending on the scale at which it is needed – could be difficult to integrate a variety of security measures together. |
| **NIST Cybersecurity Framework** | Overarching approach covering all aspects of a business or organisation. | Requires a significant cost with regards to capital, time and resources to implement and maintain. |
| Developed in collaboration with academics, industry leaders, and governmental bodies. | Requires a high level of coordination between departments in an organisation, potentially opening to risks because of communication problems. |
| Risk-based management, allowing for organisations to adapt their security strategies to meet evolving threats. | No certification to showcase adherence to the framework – could potentially prevent other businesses or parties from working collaboratively with the organisation. |
| **CIS Control Framework** | Relatively simple framework to understand by those who do not have a background in Information Technology. | Particularly resource intensive – organisations may have to invest significant amounts of time, manpower, and money to implement the framework. |
| Critical nature of the framework allows for organisations to stay up to date with regards to cyber threats. | Potential of complexity – although the framework is designed to be understood by those with no experience, many workers may be overwhelmed with what they are faced with. |
| Framework controls derived from real attack data – ensures the effectiveness of the framework for the business. | May suffer from needing to be supplemented by other security frameworks or strategies – the *CIS Control* framework does not cover protection surrounding regulations or cover for specific industries. |
| **NCSC Cyber Essentials Framework** | Opens possibilities to work with government bodies and to receive contracts from certain departments due to the UK Government backing the framework. | Higher costs if the organisation seeks to implement the *Cyber Essentials Plus* framework. |
| Low-cost to implement and maintain the basic *Cyber Essentials* framework. | Does not cover all aspects of cybersecurity – lack of processes around managing risks, and incident responses. |
| Certified framework – organisations with a security strategy using this framework will receive certification from the UK Government. | Limited, non-holistic scope of security in general – does not cover physical security or social engineering, to name but a few. |

*Table 3.2, Analysis of Cybersecurity Framework*

# 4.0 Project Specification

## 4.1 Project Objective

The initial objective of this research project is to analyse and evaluate the already existing security strategies of case study football clubs who have agreed to participate in this research project. The security strategies will be evaluated and then, using the newly developed hybrid cybersecurity framework which was also developed as part of this research project, will be used to improve the case studies overall security. The objectives of this project can be split into the following:

1. Analysis and evaluation of security strategies used by case studies to identify gaps in their existing security strategies:
   1. Beginning with a Risk Assessment to evaluate already existing security strategy
   2. Undertaking a Gap Analysis to locate and identify any gaps that may exist in said security strategy.
2. Interviews will take place with those case studies who have agreed to participate in this research project to help identify and learn more about their security strategies and identify the areas in which improvements are necessary.
3. Identify recommendations based on the gaps identified through the Gap Analysis, to improve the case studies overall security and protection. Recommendations will be suggested via the analysis discovered through the implementation of the hybrid cybersecurity framework.

## 4.2 Project Methodology

### 4.2.1 Project Research Design

With regards to the research design of this research project, a methodology of using case studies will be utilised. This will allow for the researcher to undergo a robust evaluation of the security strategies used by the case studies who have agreed to take part in the research project. Being able to identify the key areas of protection, and where little to no protection is given, will be vital in the development of this project.

### 4.2.2 Project Data Collection

A qualitative method of data collection was chosen by the researcher for this project. The researcher believes that conducting interviews with the relevant parties from the case studies will allow for a comprehensive and robust analysis of the already existing security strategies used by said case studies.

Following this, interviews allow for the researcher to provide a walkthrough of the developed hybrid cybersecurity framework to help bridge any gaps that may arise during the initial security strategy evaluation.

### 4.2.3 Project Data Analysis

A qualitative method of data analysis was chosen by the research for this project. The researcher believes this method of data analysis would be of most use when analysing the needs and requirements of the case studies. The qualitative data analysis will be split into two different sections:

1. The ***Gap Analysis***, where gaps in already existing security strategies will be identified.
2. The ***Recommendations***, where recommendations will be made to bridge the gaps in the previously analysis, based on the parameters set out by the developed cybersecurity strategy.

### 4.3.4 Project Functional Requirements

While making progress towards answering the research questions of this research project, one of the biggest aims is the creation of a hybrid cybersecurity framework that will provide football clubs with a high level of protection from cyberattacks and cybercriminals.

To answer the research questions, it was important to create a table of functional requirements to showcase what is required of this research project. To do this, *MoSCoW, or Must Have, Should Have, Could Have, Won’t Have,* prioritisation was utilised. This method of showcasing the functional requirements was chosen as it easily displays how essential and desirable certain requirements are with regards to achieving the objectives of this research project (ProductPlan, 2024).

The below table, *Table 4.1,* provides an overview of the *MoSCoW* prioritisation. It is important to note that each function will be categorised as technical or practical, allowing for the reader to easily identify which are of this research project is referring to. The ***Technical*** category refers to the hybrid cybersecurity framework, whereas the ***Practical*** category refers to the practical website used to showcase the results upon the completion of this research project:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Identifier** | **MoSCoW** | **Category** | **Description** | **Requirements** |
| **1** | **Must Have** | Technical | Essential features of the research project to achieve the research objectives and questions | Analysis of already-existing cybersecurity frameworks in order to evaluate the advantages and disadvantages of each. |
| **2** | Technical | Development of a hybrid cybersecurity framework using the best aspects of the previously discussed cybersecurity frameworks. |
| **3** | Technical | Analysis of the gaps in case studies security strategies using the newly developed cybersecurity framework. |
| **4** | Technical | Recommend improvements to security strategies of case studies in order to bridge the discovered gaps. |
| **5** | Practical | Results will be showcase on a practical website where users can analyse results for themselves. |
| **6** | **Should Have** | Technical | Features that will enhance the overall final product through the development of this research project | Ease of implementation to other sporting organisations. |
| **7** | Technical | Direct case studies to free and open-source resources to further improve security strategies. |
| **8** | Practical | Ability for users of website to use the hybrid cybersecurity framework for their own use. |
| **9** | Practical | Dynamic website allowing users to fill out risk assessment/gap analysis for themselves |
| **10** | Practical | Database functionality for website to store information submitted by users. |
| **11** | **Could Have** | Technical | Optional features that may provide added value to the research project. | Comparisons made between hybrid cybersecurity framework and industry standard ISO 27001 framework. |
| **12** | Technical | Further analysis of existing cybersecurity frameworks to further enhance the hybrid cybersecurity framework. |
| **13** | Practical | Dynamic website allowing users to gain further information surrounding each aspect of the hybrid cybersecurity framework. |
| **14** | Technical | Offer full assistance in the implementation of the recommendations of security improvements discovered throughout this project. |
| **15** | **Won’t Have** | Technical | Features that will not be added to this research project due to a variety of different reasons. | Future reviews and meetings with case studies to analyse the security strategies post-implementation of the hybrid cybersecurity framework. |
| **16** | Technical | Overall certification from any governing body. |
| **17** | Practical | Further readings or access to further security resources. |

*Table 4.1, Project Functional Requirements*

*Figure 4.1, Project Functional Requirements, showcasing the split between requirements*

## 4.3 Issues Surrounding Legality, Ethics, Society and Professionalism

Throughout the development of this research project, it was important to ensure that the research undertaken was done so in a responsible manner, complying with standards set out in a legal and ethical sense, but also ensuring it was undertaken in a professional manner that does not breach any existing societal issues.

### 4.3.1 Issues Surrounding Legality

One of the biggest areas of legality that was dealt with throughout this research project is that of data protection. The researcher has ensured the research undertaken here complies with regulations set forth by the government of the United Kingdom, namely the *Data Protection Act 2018* (UK Government, n.d.). By following this regulation, it was important to ensure information obtained from case studies was used fairly and lawfully, and for a specified purpose.

To ensure the above regulation was adhered to, the case studies who agreed to take part in the project were anonymised to ensure their names, and information surrounding their security strategies, were kept confidential.

During the first meetings with the case studies, the researcher set forth the requirements to participate in the research project, and laid out where information will be stored, what will be done with the information, and to what extent they will be anonymised throughout the research project. All contact made with the case studies was done so through the researcher’s student email address.

Information received by the researcher was stored on their own personal computer, which is protected by password protection and two-factor authentication. Correspondence between the researcher and case studies via email was also protected by password protection and two-factor authentication. To ensure compliance with GDPR, the data was stored for a limited period for the purpose of this project, after which it was disposed of.

### 4.3.2 Issues Surrounding Ethics

The biggest ethical issue that needed to be addressed throughout this research project is that of ensuring the protection of information that involved the case studies who have chosen to take part in the project. As previously mentioned in the previous sub-chapter, participants were laid out with clear information surrounding what will be done with their information, ensuring anonymity throughout the research project, ensuring no readers will be able to tell who they are just by looking at the information. To further enhance confidentiality, interviews and questionnaires were utilised as tools of assessment rather than accessing the case studies own documents that may be perceived as confidential. Emphasis was also placed on the security of information the researcher held on the case studies.

An ethical concern also arose around idea that current industry practices are spoken of, and so malicious actors may make use of said practices. This was mitigated, however, through the limited release of this project.

### 4.3.3 Issues Surrounding Society

Social issues are at the forefront of any research project, and this project is no different. A variety of issues could arise from the case studies confidentiality being broken – these case studies run the risk of a massive loss of revenue and serious damage hitting their brand and reputation. Not only this, a breach of data may also invite cybercriminals from taking advantage of a brand they now know have flaws in their security strategies.

To ensure issues surrounding society were dealt with, it was important to ensure adherence to the ethical professionalisms expected of a research project, ensuring the anonymity of the case studies to build a level of trust and transparency between the researcher and the research subjects taking part in this research project.

### 4.3.4 Issues Surrounding Professionalism

It was important for the researcher to treat this research project as if it was an important project within the workplace, and so steps were taken to ensure the researcher met a specific level of conduct when it came to professionalism. With regards to professionalism, specific issues were considered throughout this project, based on the code of conduct set forth by *The Chartered Institute for IT* known as *The* *British Computing Society* (2024)*,* as follows:

* **Issues of Competency**: It was important for the researcher to showcase a certain level of competency when undertaking this research project. Utilising the skills learned throughout the MSc degree, as well as skills that were previously developed, were of utmost importance throughout the formation of this project – combining key research skills with the newly founded knowledge was clinical not only when writing this report, but also during meetings with the case studies who agreed to take part.
* **Issues of Impartiality:** With any research project in any discipline, it was important for the researcher to remain impartial throughout. Steps were taken to expand the researcher’s knowledge base to prevent any potential bias that may occur throughout this project. This expansion of knowledge combined with the researchers already existing skills were crucial to ensuring this research project was free of any prejudice or bias.
* **Issues of Respect:** It was also important to the researcher to treat the case studies and their brands with respect through the formation of this research project. Treating them as equals allowed for the researcher to receive an honest and balanced discussion with them. Furthermore, ensuring the case studies were anonymised and data was stored securely throughout the project also ensured a high level of respect was given to the relevant parties.

Following the standards set forth by the BCS code of conduct allows for a high level of integrity in the work taking place, and so it was of utmost importance for the researcher to adhere to the code.

## 4.4 Problems, Risks and Limitations

It is important to note that, just like any other research project in any other discipline, the research does not come without problems, risks or limitations that may arise throughout the development and research process. Some problems that occurred throughout the development of this research project are as follows:

* **Problems of Sampling**: Case studies were contacted directly regarding taking part in this research project. It was not possible to get in contact with the international, mainstream football clubs, so those from lower leagues were used throughout this project – this has led to a limiting of diversity as lower league football clubs will, obviously, have a totally different experience than the world recognised brands. Risks also arose around sampling, as the football clubs chosen may not be representative, and may just want advice or to show-off.
* **Problems of Communication**: Problems arose regarding communication with the case studies, as the project was very reliant on their ability as opposed to the researchers. The researcher made attempts to alter their schedule to best fit the needs of the case studies participating in the project.
* **Problems of Information**: As with any research project, problems of information arose that were quickly dealt with by the researcher – mostly surrounding how best to store the information. The researcher ensured information and data were communicated between parties via secure channels, and said information was stored securely on the researcher’s private computer, while also making it clear to the case studies that this was the case.

# 5.0 Overall Project Design and Implementation

As stated throughout this research project, the hybrid cybersecurity framework has taken the strengths from the previously discussed already existing frameworks and integrated them into a robust and adaptable security strategy. The finished product combines aspects from the following frameworks:

* Securiti Qatar 2022 FIFA World Cup Cybersecurity Framework (**SQ**)
* NIST Cybersecurity Framework (**NIST**)
* CIS Controls Framework (**CIS**)
* NCSC Cyber Essentials Framework (**NCSC**)

Inspiration will also be taken from the NIST Cybersecurity Framework (2024), utilising most of the framework’s original category definers:

* Identify
* Protect
* Detect
* Respond
* Recover

The finished product will be showcased in a table format in the following sub-chapter, with definitions and importance ranking for each requirement identified throughout; said importance ranking will be on a scale of low, medium, to high. To provide a more in-depth analysis during the gap analysis stage, a number scale will be attached to the importance rankings, with low equating to 1, medium equating to 2, and high equating to 3. A requisite of high importance is an essential requisite a business should adhere to, while a requisite with a medium importance defines a requisite that could be implemented if resources allow. Finally, a low importance requisite defines a requisite that may not be entirely necessary but would be nice to improve the robustness of the security.

The hybrid cybersecurity framework consists of 35 key requisites that are vital to ensure the protection of a business, their information, and their assets. This combination of requisites is optimal as it covers the most important areas of which football clubs must be security-focused to ensure ideal protection. Some security concerns have been excluded, such as some aspects of physical security, due to resource and time constraints – the researcher thought it best to mostly focus on digital aspects. This does, however, open the framework to expansion in the future. The final design is as follows:

## 5.1 Design of Hybrid Cybersecurity Framework

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Category** | **Ref** | **Original Framework** | **Requisite** | **Definition** | **Importance** |
| **Identify** | I1 | NIST | Inventory of assets. | Allows for a business to keep record and monitor all assets under their umbrella. | High |
| I2 | NIST | Understanding of business role, and critical functions that support operations. | Allows for business employees to understand what the business does and what it aims to do. | Medium |
| I3 | NIST | Identify stakeholders and roles with regards to cybersecurity. | Allows employees to understand their roles within the business. | Medium |
| I4 | CIS | Establish cybersecurity policies. | Ensures businesses and their employees are aware of policies that must be adhered to. | High |
| I5 | CIS | Define responsibilities for personnel with regards to cybersecurity. | Ensures relevant personnel are aware of what is expected of them. | Medium |
| I6 | CIS | Periodic reviews of policies and procedures. | Ensures policies and procedures are up-to-date and industry standard. | Medium |
| **Protect** | P1 | CIS | Implement role-based access controls. | Ensures only relevant personnel can access the necessary areas. | High |
| P2 | NCSC | Implement two-factor authentication system. | Ensures a further layer of protection covering assets. | High |
| P3 | NCSC | Implement encryption on necessary assets. | Ensures a further layer of protection covering assets. | High |
| P4 | NCSC | Periodic reviews of access controls. | Ensures personnel who no longer need access to certain areas can no longer do so, and vice versa. | Medium |
| P5 | NIST | Implement data encryption. | Ensures data and information is protected and secure. | High |
| P6 | NIST | Implement data handling policies. | Ensures personnel know how to handle data and what to do with it. | Medium |
| P7 | CIS | Periodic backing up of data. | Ensures data is protected if a detrimental action were to occur. | Medium |
| P8 | NCSC | Regular cybersecurity training for all staff members. | Ensures personnel are aware of cybersecurity risks and what is expected of them. | Medium |
| P9 | NIST | Implement VPN software. | Ensures devices are protected when used on foreign networks. | High |
| P10 | NIST | Implement device protection software, including firewalls and anti-malware software. | Ensures devices are protected from malicious acts from occurring. | High |
| P11 | NIST | Periodic updates of device protection software. | Ensures devices are protected from new and modern risks. | High |
| P12 | NCSC | Secure disposing of devices and data that are no longer required. | Ensures data and devices do not fall into the wrong hands. | Medium |
| **Detect** | D1 | SQ | Implement systems to monitor traffic on network systems and user systems. | Helps to track suspicious activity, including identifying the source. | High |
| D2 | SQ | Implement SIEM (Security Information and Event Management) systems to correlate logs. | Helps to prevent security threats from exploited vulnerabilities. | Medium |
| D3 | CIS | Develop detection procedures. | Helps personnel to understand their responsibilities when an anomaly is detected. | Medium |
| D4 | CIS | Periodic exposure assessments. | Helps to expose any vulnerabilities and fixes them. | Medium |
| D5 | CIS | Periodic penetration testing. | Helps to expose any vulnerabilities and fixes them. | Medium |
| D6 | CIS | Implement anomaly detection software. | Helps to expose any anomalies that may breach the network. | Medium |
| **Respond** | RS1 | SQ | Creation of an incident response plan. | Ensures personnel are aware of what to do during an incident. | High |
| RS2 | SQ | Definition of roles and responsibilities during an incident. | Ensures personnel are aware of their own responsibilities during an incident. | Medium |
| RS3 | NCSC | Implement containment and eradication processes. | Processes to ensure incidents are isolated and eradicated to continue protection. | Medium |
| RS4 | NCSC | Implement software to isolate issues. | Ensures issues do not spread to other areas of the business. | Medium |
| RS5 | SQ | Creation of communication routes for stakeholders during incidents. | Ensures stakeholders are aware of incidents occurring and steps taken to remediate. | Medium |
| RS6 | SQ | Creation of templates to be utilised as status indicators. | Ensures continuous updates are given when dealing with incidents. | Low |
| **Recover** | RC1 | NIST | Creation of recovery plan to establish systems and data. | Ensures steps are in place to resume business activity. | High |
| RC2 | NIST | Periodic testing of recovery processes. | Ensures recovery processes are working and up to date. | Medium |
| RC3 | NIST | Analysis of reports after incidents occur to understand problems. | Allows relevant personnel to gain an insight into the problems that have occurred. | High |
| RC4 | NIST | Update policies based on the analysis of reports. | Ensures the best protection is given to the organisation. | High |
| RC5 | SQ | Communication of recovery steps to stakeholders. | Ensures stakeholders are aware of the steps being taken to remediate problems. | Medium |

*Table 5.1, Hybrid Cybersecurity Framework Design*

*Figure 5.1, Split of Hybrid Cybersecurity Framework Categories*

*Figure 5.2, Structure of Hybrid Cybersecurity Framework*

The above table, *Table 5.1*, showcases the designed hybrid cybersecurity framework to be utilised by football clubs – addressing the key areas in which said sporting organisations face the biggest challenges. The next figure, *Figure 5.1,* displays the split of categories in the hybrid cybersecurity framework, while *Figure 5.2* displays the composition of the hybrid framework. It was important when developing the framework to make it easy and concise to read and understand not just by IT professionals, but also from those out with an IT team.

## 5.2 Implementation

The implementation of this newly created hybrid cybersecurity framework required cooperation with the case studies who agreed to take part in this research project. The following steps outline the actions taken to implement:

1. **Case Study Risk Assessment and Gap Analysis**: This first action, and potentially the most important, involves a comprehensive analysis of the security processes already set in place by the football club case studies who have agreed to take part in the research project. Using the newly created hybrid framework as a guide to assess the extent to which the case studies are protected, the researcher can pinpoint gaps in the current security architecture.
2. **Recommendations**: After analysing the security strategy and identifying any gaps, the researcher can provide key recommendations that will help bridge said gaps, detailing the best actions to take to ensure the best protection is given to the case studies.
3. **Final Implementation**: Following the recommendations, the researcher can work in tandem with the case studies to work on the best way to maximise resources and implement the previously recognised recommendations.
4. **Case Study Evaluation**: Finally, once the case studies have accepted the recommendations and begun the implementation phase, feedback is obtained via an evaluation questionnaire, covering areas such as the ease of which the hybrid cybersecurity framework is understood, how effective it is, and how impactful the recommendations that were suggested by the researcher are. This evaluation is crucial for allowing improvements to be made to the newly developed framework.

## 5.3 Design of Practical Website

As part of this researcher project, the researcher also decided to showcase the results from the case studies in a series of webpages. This allows for the case studies to easily reflect on the discoveries made during their risk assessment and gap analysis, and to easily pinpoint where improvements must be made to their security strategies based on the recommendations made by the researcher.

The webpages will also feature a section allowing for other football clubs to undertake their own risk assessments and gap analysis using a dynamic version of the newly created hybrid cybersecurity website. This tool will allow users to both edit and delete their inputted gap analysis as they see fit.

The following figure, *Figure 5.3*, showcases the overall flow diagram of the website being created as part of this research project:

*Figure 5.3, Website Flow Diagram*

A screenshot of a computer

Description automatically generated

*Figure 5.4, Website Index Page Wireframe*

A screenshot of a computer

Description automatically generated

*Figure 5.5, Database Design*

The researcher sought to design the webpages in a way to not cause unnecessary strain on the eyes of the user and to make it easy to understand – a simple neutral colour scheme was used to achieve this, as well as utilising a simple font while also increasing the font sizes. The researcher also implemented code to highlight sections of the table that the user is hovering over, to make clear what section they are reading by making it stand out against the rest of the table – a coral colour scheme was used as a highlighter to make it pop out.

A simplified version of the hybrid cybersecurity framework was used as part of the Gap Analysis Tool – this decision was taken to not overwhelm the user. Reference IDs were provided, allowing users to refer to the main framework to fully understand the requisites if necessary.

The researcher also sought to showcase a variety of security tools that can be used by users to improve their security architecture and become compliant with the requisites set forth by the hybrid cybersecurity framework. This was important as it allows for users to reflect on their own progress when updating their current security strategies.

The use of a relational database allows for the information inputted by the user to be stored on the back end, and recalled, edited, and deleted via the created webpages when necessary. This type of database was chosen due to its easy of scalability and understanding, as well as its general simplicity with regards to the storing of data. The rationale behind the design chosen in *Figure 5.5*, was to ensure an efficient and consistent database was created – the use of a primary key and proper indexing ensures a high level of data integrity.

To create these webpages, a combination of HTML, CSS, PHP and SQL were utilised. This combination of programming languages allows for a simple, yet effective, series of webpages and tools to be developed as part of this project.

Some implementation challenges were faced by the researcher. Issues of security were raised while designing the website – data protection suffers due to a lack of knowledge surrounding the subject. No secure encryption was utilised, and so data may be susceptible to theft via an SQL injection.

This practical website, created as part of the requirements for this MSc Research Project, is an incredibly valuable tool for not only these case studies interacted with throughout the formation of this project, but also for other football clubs and potentially even other sporting organisations that seek to improve their own security architecture. Further information surrounding this practical website can be found in *Appendix E* and *Appendix F*.

# 6.0 Findings

Using a process of semi-structured interviews with the case studies, the hybrid cybersecurity framework created was used to measure the security strategies of the case studies, and to pinpoint where gaps are present in said strategies – the following sub-chapters will showcase the overall findings, and then move on to discuss the findings from each case study.

## 6.1 Overall Findings

The following table, *Table 6.1*, presents an overview of the analysis done with the case studies, with data taken from *Appendix C*. The four case studies who agreed to take part in this research project were analysed to understand what extend they reached a target level of compliance with regards to the 35 requisites set forth in the hybrid cybersecurity framework.

The level of compliance is calculated by taking the number scale attached to the importance ranking provided in the hybrid cybersecurity framework, e.g. low importance is 1 and medium importance is 2, etc.

The table showcases the total number of each category used in the framework, the level of compliance for said category, and the level of which each case study has achieved. Finally, the final row provides the reader with a final total level of compliance across the board. To be fully compliant with the hybrid security framework, the total level of compliance for each case study must reach the level of compliance of 83.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Category** | **Requisite Total** | **Level of Compliance (LOC)** | **Case Study A LOC** | **Case Study B LOC** | **Case Study C LOC** | **Case Study D LOC** |
| **Identify (I)** | 6 | 14 | 2 | 6 | 5 | 0 |
| **Protect (P)** | 12 | 31 | 10 | 12 | 12 | 9 |
| **Detect (D)** | 6 | 13 | 2 | 2 | 3 | 3 |
| **Respond (RS)** | 6 | 12 | 4 | 6 | 3 | 4 |
| **Recover (RC)** | 5 | 13 | 5 | 5 | 2 | 3 |
| **Total** | **35** | **83** | **23** | **31** | **25** | **19** |

*Table 6.1, Overall Findings*

As previously stated, the above table, *Table 6.1*, provides an overall understanding of the gap analysis undertaken with the case studies, allowing the researcher and readers to see where improvements must be made. The following sub-chapters will provide a further analysis of each case study’s overall analysis.

### 6.1.1 Findings of Case Study A

Case Study A is a football club competing in the fourth division of the Scottish Football pyramid. Operating at a relatively high level, the case study has access to a level of financial and personnel resources higher than those below them in the football pyramid. This is reflected in the gap analysis, however plenty of gaps still arose.

*Figure 6.1, Case Study A Findings*

From the above figure, *Figure 6.1*, we can see the comparison between the necessary level of compliance, and the actual level of compliance from Case Study A. We can clearly see that Case Study A is severely lacking with regards to complying with the requisites set forth by the hybrid cybersecurity framework – the highest level of compliance can be seen in the protect category, and the lowest in the identify and detect categories, however by combining the scores, we can see that the case study only adheres to a level of 23 out of the 83 required to be fully compliant; a mere 27.7% adherence percentage.

### 6.1.2 Findings of Case Study B

Case Study B is a football club competing in the second division of the Scottish Football pyramid. Ranked higher in the leagues than the other case studies chosen to take part in this research project, this case study has access to more resources than the others, on both a financial and personnel level – this is clearly reflected in the gap analysis undertaken.

*Figure 6.2, Case Study B Findings*

*Figure 6.2* shows us a comparison between the necessary level of compliance and the level of compliance reached by Case Study B. We can clearly see an improvement in these levels compared to that of Case Study A, with improvements across all categories – particularly in the identify, respond, and recover categories, respectively. However, necessary improvements must still be made, as only a level of 31 out of 83 has been reached; only 37.3% adherence percentage.

### 6.1.3 Findings of Case Study C

Case Study C is another football club competing in the fourth division of the Scottish Football pyramid. This case study operates in a similar manner to that of Case Study A, and so the gap analysis reflects a similar outcome to said case study.

*Figure 6.3, Case Study C Findings*

*Figure 6.3* provides us with a comparison between the necessary level of compliance and the level achieved by Case Study C. When compared to that of Case Study A, we can see very similar results – not too much of a surprise as both case studies are very similar in nature. Case Study C sees improvements in the identify, protect and detect categories, but does fall short in the respond and recover categories when compared to the latter. When a combination of the scores is undertaken, a level of 25 out of 83 is achieved; a 30.1% adherence percentage.

### 6.1.4 Findings of Case Study D

Case Study D is a football club competing in the Highland Football League, in the fifth division of the Scottish Football pyramid. Playing at a lower level in the league system than the other case studies, resources are scarcer for this case study, reflected in the gap analysis.

*Figure 6.4, Case Study D Findings*

*Figure 6.4* provides us with a comparative analysis of the necessary level of compliance and the level reached by Case Study D. As previously stated, Case Study D is operating at the lowest level amongst the case studies chosen to take part in this project, and this is clearly reflected in the findings. Case Study D is non-compliant with regards to all requisites in the identify category but is also not too dissimilar with regards to the other categories, and even having an equal to or higher compliance level with the detect categories than the other case studies. Combining the scores presents us with a level of 19 out of 83; a small adherence percentage of 15.8%

## 6.2 Summary of Findings

To summarise the findings discovered from the case study gap analysis’s, we can clearly see that the practicing of good cybersecurity hygiene is not something that is commonplace in the world of football. No case study achieved an adherence score of above 40%, with even one case study being as low as 15.8% - we can clearly see that these football clubs are at risk of being preyed upon by cybercriminals.

The below figure, *Figure 6.5*, provides an easy-to-understand summary of just how far not just these case studies, but football clubs, need to go in order to be fully protected and obtain a high level of cybersecurity hygiene that encompasses not just information, but also the people and the assets of the business.

*Figure 6.5, Summary of Findings*

However, we must acknowledge that these case studies are not the biggest names on the world stage of football, and so the resources available to them are finite. Looking back at *Figure 6.5*, we can clearly see that Case Study B has the highest adherence level – this makes sense as they are higher up in the Scottish Football Pyramid, and so have access to more resources and capital. From this, we can make an educated guess and argue that the household names in football would most definitely have a higher level of compliance when undergoing a risk assessment and gap analysis via this hybrid cybersecurity framework.

It is also important to note which themes had a reoccurring nature while undertaking this research:

* Case Studies did not know what cybersecurity frameworks were and the benefits and protection they could bring to the football club. This is clearly reflected in the gap analysis, where no case study came close to being fully compliant.
* Most Case Studies did not have dedicated IT personnel, with members of staff pitching in wherever necessary.
* Lack of IT training, particularly cybersecurity, increasing the risk at which attacks could take place.
* Lack of resources to implement protection with regards to cybersecurity – because of this, the case studies deemed the protection to not be a priority to continue business operations.
* Case Studies hold the “*but who would want to attack us?”* belief, further enhancing the idea that cybersecurity is not the biggest priority.

It is important for these themes to be understood so solutions can be communicated to the relevant parties when introducing cybersecurity to their operations – a robust and overarching approach must be taken to ensure the best protection is given to the organisations.

# 7.0 Conclusions

## 7.1 Case Study Evaluations

To gain feedback surrounding the hybrid cybersecurity framework and its implementation, the case studies chosen to take part in this project were asked to fill out an evaluation document. This document sought to understand the extent to which the case studies understood cybersecurity, their understandings of the hybrid framework, and their understandings of the frameworks impact.

A general overview of the evaluation document, found at *Appendix D*, is as follows:

* The case studies provided a rating of 4 out of a possible 5 for the hybrid cybersecurity framework, citing its ease of understanding for the most part to be important.
* 3 of the case studies found the hybrid cybersecurity framework easy to understand and appreciated the simplicity of its designs. However, the fourth case study did find some of its aspects a bit confusing.
* All the case studies believed that the implementation of the hybrid cybersecurity framework would improve their cybersecurity hygiene.
* All the case studies believed that the hybrid cybersecurity framework allowed for their teams to gain a better understanding and a different perspective to key cybersecurity practices.
* All the case studies have begun to implement some of the recommendations set out by the hybrid cybersecurity framework. Some of the case studies acknowledge that this may take time and may not be able to implement every recommendation simply due to resource constraints.
* Some of the case studies acknowledged that some terms used in the hybrid cybersecurity framework were not immediately understood and sought further guidance from the researcher. Some of these terms included *encryption* and *SIEM systems.*
* Some of the case studies acknowledged that some aspects of the hybrid cybersecurity framework were, or are, too difficult to implement. The main reasoning behind this was a lack of resources.
* All the case studies would recommend the hybrid cybersecurity framework to other parties in the industry and beyond, citing the ease of understanding and overall coverage to be areas of excellence.

## 7.2 Limitations

As with every research project, this project is no stranger to several limitations that hindered the overall effectiveness the work. Some of these limitations are as follows:

* Case studies were not contacted again regarding how effective the implementation of recommendations was, simply due to time constraints during the development of this project.
* The hybrid cybersecurity framework created as part of this project was not compared with other world-leading standards of security, such as ISO 27001, and so gaps or improvements could not be filled and made.
* The hybrid cybersecurity framework utilised general terms for all its requisites and was not expanded upon. This is due to the small sample size and quality of the samples.
* The hybrid cybersecurity framework was only composed of four different already existing frameworks – arguments could be made that including further frameworks could lead to a more robust and comprehensive hybrid framework.
* No requisites revolved around laws or regulations of countries were added to the hybrid cybersecurity framework. The addition of these would allow for a more comprehensive approach.

It is important to identify how some of these limitations could be overcome. The researcher believes that if additional time and resources were spent on the hybrid cybersecurity framework, then it would become a more robust tool. In doing so, comparisons can also be made with information security world standards, and dialogue could be started with the relevant governmental bodies to ensure further requisites were added.

## 7.3 Recommendations

The purpose of this research project was to create a hybrid security framework to be used by football clubs, to improve their cybersecurity hygiene. From understanding the findings and overall analysis of the case studies, several recommendations are set forth by the researcher:

* Football clubs, and other sporting organisations, should ensure that a robust cybersecurity strategy is part of their business plan; allocating resources where necessary and ensuring training is given to all employees.
* Football clubs should hire dedicated IT personnel to oversee their security strategy. If this is not feasible, resources should be allocated to ensure relevant parties are aware of what is expected of them.
* Football clubs should utilise security tools such as encryption technology and antimalware technology to enhance cybersecurity hygiene.
* Football governing bodies, such as the SFA and UEFA, should allocate resources to educate football clubs across the football pyramid on the dangers of cyberattacks.
* Football clubs should ensure that all employees, including staff, players, and volunteers, should have their workplace devices protected by the standards set out in the hybrid cybersecurity framework.

## 7.4 Recommendations for Future Work

This research project sets a good foundation for further research to be undertaken with regards to cybersecurity in football. However, it does not reach far enough, and so further work must be undertaken. Some recommendations for future work are as follows:

* Increasing sample sizes to include ‘larger’ football clubs, and football clubs around the world, would increase the diversity of the findings and the overall analysis undertaken throughout.
* Future work could revolve around the use of cloud computing and technologies in the world of football and sport in general. An ever-growing field of technology, many sporting organisations are beginning to rely on cloud computing to grow their businesses.
* Future work could seek to understand the importance of governmental bodies with regards to cybersecurity in football, or other sporting organisations.
* Finally, future work could also seek to understand the effectiveness of free security technologies, and how they compare to security technologies that may have an increased cost on a resource and financial level.

# References

ADLER, S. (2020) *IOTW: World’s Third Most Valuable Football Club Hit by Cyber Attack.* [online] London: Cyber Security Hub. Available from: <https://www.cshub.com/attacks/articles/worlds-third-most-valuable-football-club-hit-by-cyber-attack> [accessed: 18/06/2024]

AL-DOSARI, K., et al. (2023) *Security Supply Chain Using UAVs: Validation and Development of a UAV-Based Model for Qatar’s Mega Sporting Events*. Drones. 7 (9)

ANDJELIC, S., DOYLE, C. & HOSSAIN, G. (2022) *Cybersecurity Risk with Wearable Technology in Sports: Why Should We Care?* 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET). 160-165

BADA, M. & NURSE, J. R. C. (2019) *Developing Cybersecurity Education and Awareness Programmes for small- and medium-sized enterprises (SMEs).* Information and Computer Security.

BAKER, F. C. (2021) *Inadequacy of Existing Security Management Frameworks in Addressing Internet of Things*. [online] PhD: Northcentral University. Available from: <https://www.proquest.com/openview/7ef49841802d54fff144083abf64a855/1?pq-origsite=gscholar&cbl=18750&diss=y> [accessed: 20/06/2024]

BRITISH COMPUTING SOCIETY*.* (2024) *BCS Code of Conduct*. [online] London: British Computing Society. Available from: <https://www.bcs.org/membership-and-registrations/become-a-member/bcs-code-of-conduct/> [accessed: 25/06/2024]

CARBIDE. (2024) *How to Use the CIS Controls Framework for Your Business*. [online] Cape Breton: Carbide. Available from: <https://carbidesecure.com/resources/how-to-use-cis-security-framework/> [accessed: 19/06/2024]

CENTRE FOR INTERNET SECURITY. (2024) *CIS Critical Security Controls.* [online] East Greenbush: Centre for Internet Security. Available from: <https://www.cisecurity.org/controls> [accessed: 19/06/2024]

COLON, M. (2024) *Breaking Dwon the Intersection of AI and Cybersecurity*. [online] Bucharest: Bitdefender. Available from: <https://www.horangi.com/blog/real-life-examples-of-web-vulnerabilities> [accessed: 22/06/2024]

CRAWLEY, K. (2021) *8 Steps to Better Security: A Simple Cyber Resilience Guide for Business*. Hoboken: John Wiley & Sons

GAUGHAN, J. (2016) *London Stadium trespassers will not face prosecution despite breaking into West Ham’s stadium*. [online] London: Mail Online. Available from: <https://www.dailymail.co.uk/sport/football/article-3827266/London-Stadium-trespassers-not-face-prosecution-despite-breaking-West-Ham-s-stadium.html> [accessed: 18/06/2024]

GROW, N. & SHACKELFORD, S. J. (2020) *The Sport of Cybersecurity: How Professional Sports Leagues Can Better Protect the Competitive Integrity Of Their Games*. Boston College Law Review: Kelley School of Business Research paper No. 19-14.

IT GOVERNANCE. (2024) *The Cyber Essentials Scheme*. [online] Cambridge: IT Governance. Available from: <https://www.itgovernance.co.uk/cyber-essentials-scheme> [accessed: 19/06/2024]

KIDD, C. (2023) *CIA Triad: Confidentiality, Integrity & Availability*. [online] San Jose: Splunk. Available from: <https://www.splunk.com/en_us/blog/learn/cia-triad-confidentiality-integrity-availability.html> [accessed: 18/06/2024]

MALIK, O. I. (2024) *Understanding FIFA 2022 World Cup Cybersecurity Framework*. [online] San Jose: Securiti. Available from: <https://securiti.ai/blog/understanding-fifa-2022-world-cup-cybersecurity-framework/> [accessed: 19/06/2024]

MANSON, D. & PIKE, R. (2014) *The Case for Depth in Cybersecurity Education*. ACM Inroads. 5 (1): 47-52

MARTIN, A. (2024) *French football club PSG says ticketing system targeted by cyberattack*. [online] Somerville: The Record. Available from: <https://therecord.media/paris-saint-germain-cyberattack-ticketing-system> [accessed: 18/06/2024]

MOSCHOVITIS, C. (2018) *Cybersecurity Program Development for Business: The Essential Planning Guide.* Hoboken: John Wiley & Sons

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2024) *Frequently Asked Questions*. [online] Gaithersburg: National Institute of Standards and Technology. Available from: <https://www.nist.gov/cyberframework/faqs> [accessed: 19/06/2024]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (2024) *The NIST Cybersecurity Framework (CSF) 2.0.* [online] Gaithersburg: National Institute of Standards and Technology. Available from: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf> [accessed: 19/06/2024]

OSBORNE, B. (2017) *Legal and Ethical Implications of Athletes’ Biometric Data Collection in Professional Sport*. Marquette Sports Law Review. 28 (1)

OYELEKE, S. (2021) *Sergio Aguero, 16 other popular footballers who suffered heart problems.* [online] Lagos: The Punch. Available from: <https://punchng.com/sergio-aguero-16-other-popular-footballers-who-suffered-heart-problems/> [accessed: 10/07/2024]

PAGE, M. J., et al. (2021) *The PRISMA 2020 statement: an updated guideline for reporting systematic reviews*. Research Methods & Reporting. 372 (71)

PATTERSON, J. (2017) *Cyber-Security Policy Decisions in Small Businesses*. [online] PhD: Walden University. Available from: <https://www.proquest.com/openview/ff68c91e2ca67e6a45ac1f6486dcf5ff/1?pq-origsite=gscholar&cbl=18750> [accessed: 10/07/2024]

PELZER, L. M. (2021) *The True Cost of Cybersecurity Incidents: The Problem*. [online] Santa Clara: Palo Alto Networks. Available from: <https://www.paloaltonetworks.com/blog/2021/06/the-cost-of-cybersecurity-incidents-the-problem/> [accessed: 08/07/2024}

PRISMA. (2024) *PRISMA 2020.* [online] Clayton: PRISMA. Available from: <https://www.prisma-statement.org/> [accessed: 02/07/2024]

PRODUCTPLAN. (2024) *MoSCoW Prioritisation*. [online] Denver: ProductPlan. Available from: <https://www.productplan.com/glossary/moscow-prioritization/#:~:text=MoSCoW%20prioritization%2C%20also%20known%20as,will%20not%20have%20right%20now> [accessed: 02/07/2024]

RAWASS, J. (2019) *Cybersecurity Strategies to Protect Information Systems in Small Financial Institutions*. [online] PhD: Walden University. Available from: <https://www.proquest.com/openview/618fd7212e04c579fbac277a31d38353/1?pq-origsite=gscholar&cbl=18750&diss=y> [accessed: 13/07/2024]

SAMONAS, S. & COSS, D. (2014) *The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security*. Journal of Information System Security. 10 (3)

SECURITI. (2024) *Qatar DPL*. [online] San Jose: Securiti. Available from: <https://securiti.ai/solutions/qatar-dpl/> [accessed: 19/06/2024]

SELOOM, M. (2024) *Qatar’s Security Strategy in the 2022 FIFA World Cup.* [online] Doha: Doha Institute for Graduate Studies – College of Social Sciences and International Studies. Available from: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4712971> [accessed: 19/06/2024]

SILL, Y. (2023) *Cybersecurity resources for Small and Medium-Sized Businesses*. [online] MSc: Utica University. Available from: <https://www.proquest.com/openview/90561789383bdeed5c8064a366052768/1?pq-origsite=gscholar&cbl=18750&diss=y> [accessed: 11/07/2024]

THORPE, J. (2024) *FC Barcelona names Official Cybersecurity Partner*. [online] Cambridge: International Security Journal. Available from: <https://internationalsecurityjournal.com/fc-barcelona-cybersecurity-partner/> [accessed: 26/06/2024]

UK GOVERNMENT CABINET OFFICE. (2023) *PPN 09/23: Updates to the Cyber Essentials Scheme*. [online] London: UK Government. Available from: <https://www.gov.uk/government/publications/ppn-0923-updates-to-the-cyber-essentials-scheme> [accessed: 19/06/2024]

UK GOVERNMENT. (n.d.) *Data Protection*. [online] London: UK Government. Available from: <https://www.gov.uk/data-protection> [accessed: 20/06/2024]

# Appendices

## Appendix A – Project Log

Throughout the development of this project, the researcher was eager to get going and complete the project in a timely manner. A rough plan was made to be followed to ensure this was the case, showcased here in *Table B.1*:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Task** | **Week Commencing** | **Timeframe** | **Status** | **Notes** |
| Project Formulated | 10/06/2024 | 1 week | Completed | - |
| Introduction | 17/06/2024 | 1 week | Completed | - |
| Literature Review | 17/06/2024 | 2 weeks | Delayed Completion | Delayed completion due to addition of further information |
| Project Specification | 24/06/2024 | 1.5 weeks | Completed | - |
| Case Studies Contacted and Evaluated | 24/06/2024 | 3 weeks | Completed | Some contact kept with case studies to ensure progress is continued |
| Design and Implementation | 01/07/2024 | 2 weeks | Completed | - |
| Findings | 08/07/2024 | 1 week | Completed | - |
| Conclusions | 08/07/2024 | 1 week | Completed | - |
| Finalise Report | 15/07/2024 | 0.5 weeks | Completed | - |
| Practical Website Component | 22/07/2024 | 2 weeks | Completed | - |
| Academic Poster | 29/07/2024 | 1 week | Completed | - |

*Table B.1, Project Log*

The above information in *Table B.1* was composed by collating the information from the *Project Weekly Reports* that were submitted every week as part of the module requirements.

The researcher was keen to finalise everything in a quick and timely manner – this was easily achieved as the researcher had no other commitments during this time and was able to focus to the best of their ability.

The researcher acknowledges that the timely completion of the work undertaken with case studies may have been different had the sample contained case studies of a different nature. This is something that must be considered if further work is undertaken in this area.

## Appendix B – Call for Case Studies & Further Discussions

With the intention of recruiting case studies to participate in this research project, the researcher made contact with several different football clubs in Scotland to gauge interest in taking part. The following email, *Figure B.1,* was sent to said football clubs, with details surrounding what is required, and how to get in touch with the researcher:

A screenshot of a computer

Description automatically generated

*Figure B.1, Call for Case Studies*

Several football clubs were contacted regarding participating, and a total of four agreed to take part in the formation of this project.

After receiving agreements to participate in the project, the researcher sent the following email to organise a date and time to hold a meeting, seen here in *Figure B.2*:

A screenshot of a computer

Description automatically generated

*Figure B.2, Organisation of Meeting*

The researcher had no difficulties in organising meetings with the case studies and was able to hold all of them the following week (week commencing 01/07). Following the meetings with the case studies, the researcher sent an email summarising the key points that were discussed, and a reminder of what will happen with their information. This can be seen here in *Figure B.3*:

A screenshot of a computer

Description automatically generated

*Figure B.3, Summary of Meeting*

## Appendix C – Gap Analysis

During the meetings undertaken between the researcher and the case studies, a gap analysis was undertaken using the newly developed hybrid cybersecurity framework. The researcher spoke through the framework with the case studies to receive the level of which they were compliant in each requisite set out by the framework.

To perform the gap analysis and analyse the level of compliance for each case study, the researcher performed the following:

* Added a numerical system to each importance ranking, as follows:
  + Low: 1
  + Medium: 2
  + High: 3
* Added a numerical system to the compliancy level, as follows:
  + Non-Compliant: 0
  + Partly Compliant: 1
  + Fully Compliant: 2
* The targeted level of compliance was calculated by multiplying the importance ranking weight with the target weight, giving parties a base number to strive towards – anything equal to this number is wholly beneficial to the case study.
* Finally, the total level of compliance for each case study was calculated by multiplying the importance ranking weight with the case study level discovered following the gap analysis.

The following figure, *Figure C.1*, is a total rundown of the analysis undertaken during the gap analysis for all case studies who took part:

A screenshot of a chart

Description automatically generated

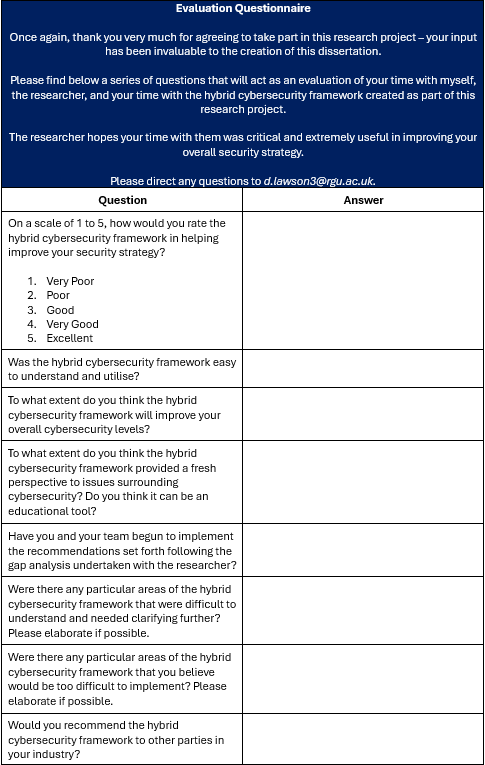
*Figure C.1, Gap Analysis*

The overall gap analysis revealed that none of the case study participants were anywhere near close to being fully complaint with the hybrid cybersecurity framework, and that an outstanding amount of work must be undertaken in order to improve the security hygiene.

As useful tools for this research project, this gap analysis, as well as the raw data sheet, have been uploaded to the final drop box.

## Appendix D – Evaluation Documentation

In order to gain some evaluation surrounding the effectiveness of the hybrid cybersecurity framework created as part of this project, an evaluation document was sent to the case studies in order to gather information surrounding their experiences and thoughts, as seen in the following figure, *Figure D.1*:



*Figure D.1, Evaluation Documentation*

Again, as a useful tool for this research project, the above blank evaluation documentation has been uploaded to the final drop box.

## Appendix E – Website Test Cases

In order to ensure the created website was working as intended, several test cases were undertaken to make note of the expected and actual results of the tests. See the below table, *Table E.1*:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test No.** | **Test Method** | **Expected Result** | **Actual Result** | **Comment** |
| **1** | All links between webpages clicked | Directed to the relevant correct webpage | Directed to the relevant correct webpage | Correct code utilised to connect webpages together |
| **2** | External links clicked | Directed to the relevant correct webpages | Directed to the relevant correct webpages | Correct code utilised to connect external webpages |
| **3** | Gap Analysis Tool submit button clicked | Information sent and stored in back-end database | Information sent and stored in back-end database | Relevant information submitted; data can be added to the database |
| **4** | Inputting of wrong name in Gap Analysis Delete Data text box | Error message | User redirected to index page | Website should display an error message instead of redirecting user |
| **5** | Inputting of correct name in Gap Analysis Delete Data text box | Inputted information deleted from database, redirected to index page | Inputted information deleted from database, redirected to index page | Correct information submitted; data removed from the database |
| **6** | Gap Analysis Tool delete button clicked | Information deleted from database, redirected to index | Information deleted from database, redirected to index | Relevant information deleted from database |
| **7** | Edit Gap Analysis link clicked | Redirected to gap analysis edit page | Redirected to gap analysis edit page | Relevant information can be edited by user |
| **8** | Inputting of correct name in gap analysis edit box | Redirects user to main edit page | Redirects user to main edit page | Allows user to edit information stored in database |
| **9** | Inputting of incorrect name in gap analysis edit box | Error message | Redirects user to main edit page | Should prevent user from reaching main edit page |
| **10** | Edit Gap Analysis submit button clicked | Redirects user to main edit page | Redirects user to main edit page | Allows user to edit information stored in database |
| **11** | Gap Analysis Tool text box filled | Text box filled | Text box filled | Correct information added to text boxes to be added to database |

*Table E.1, Website Test Cases*

## Appendix F – GitHub Repository

The code used for the webpages developed as part of this research project can be found on the researchers GitHub Repository at the following link:

<https://github.com/davidaclawson/MSc-Project.git>

Said code will also be stored in a zip file and uploaded to the final drop box.