Research and case scenario in Data Security and Compliance

ACCA5034: DATA SECURITY AND COMPLIANCE

JOE FROHWEIN | 2315545

UNIVERSITY OF WALES TRINITY SAINT DAVID

RESEARCH AND CASE SCENARIO IN DATA SECURITY AND COMPLIANCE

Joe Frohwein

Student University of Wales Trinity St David, Swansea, Wales

2315545@student.uwtsd.ac.uk

Abstract- ***Advancing into the digital era, the need for robust security systems also continues to advance, as does the escalating threat of cyber-attacks. This paper aims to highlight the importance of physical security, which is the protection of IT systems and infrastructure against unauthorised access and unplanned events, through measures such as access controls and environmental monitoring. Delving into specific forms of threats of physical loss, including threats such as extreme temperatures, liquids, living organisms and movement due to natural events, this paper aims to emphasize the need for safeguarding of IT infrastructure using varying security strategies to protect, detect, react and safeguard against all threats on all fronts, in order to ensure the integrity and reliability of their IT system, whilst maintaining a secure environment against the documented threats and risks.***

I. Introduction

As the world continues to progress and make further advancements into the digital era, the integration of robust information security systems and infrastructure has become paramount for organisations. The likelihood and impact of potential cyber security threats has also continued to advance; therefore, modern businesses must be able to maintain a secure environment.

A secure environment is one that that identifies, protects, detects, responds and recovers against any cyber threat, which are also the five functions of the National Institute of Standards and Technology's (NIST) Cybersecurity framework, which is used to "aid organizations in easily expressing their management of cybersecurity risk at a high level and enabling risk management decisions" [1], [2].

Physical security is the protection of physical items, objects, or areas from unauthorised access and misuse. This can be achieved through a series of physical access controls, such as fencing & gates, guards & dogs, ID access, locks & keys, alarms etc. These will all be elaborated upon throughout the main body of this paper.

Donn B. Parker compiled a list that he referred to as "the seven major sources of physical loss" [3], [4], which are:

- Extreme temperature
- Gases
- Liquids
- Living Organisms
- Projectiles
- Movement
- Energy anomalies

This paper explores some of these seven points, delving into the different types of robust security measures to protect against these breaches of physical security, while reviewing why modern organisations must prioritise the protection of their IT systems and infrastructure.

II. Body

A. Extreme Temperature

Extreme variations of temperature, both hot and cold, such as sunlight, fire or freezing,

can have adverse effects on IT systems and cause equipment to malfunction due to temperature damage.

For example, Jason Andress stated that "in environments that contain large numbers of computers and associated equipment, such as in a data centre, we rely on environmental conditioning equipment to keep the temperature down to a reasonable level, typically in the high-60s to mid-70s on the Fahrenheit scale" which converts to roughly to low-20s on the Celsius scale [5]. Failure to protect against these high temperatures could, in the worst-case scenario, lead to a fire. These circumstances could be prevented, and the equipment protected, using measures such as 'clean agent', carbon dioxide or gas-based fire suppression systems, monitoring systems and isolation systems [6], [7].

On the other end of the spectrum, The American National Coordinator for Critical Infrastructure Security and Resilience stated that freezing temperatures and environments can cause a wide range of damages to IT equipment and infrastructure, such as electrical equipment becoming frozen and structural collapse or roof failure of remote data/research centres due to accumulation of frozen precipitation [8]. The threat of freezing temperatures can be mitigated using measures such as "regular inspections of infrastructure, climate control systems, and the implementation of redundancy for critical components" [9].

To summarise this subsection, these sources of literature show how the extreme effects of temperature pose significant threats to IT systems and why these conditions must be monitored and safeguarded against. It also shows how the physical impact of extreme temperatures can occur at both extremes, both hot and cold. Implementing protective strategies is vital for maintaining the integrity and reliability of IT systems in varying environmental conditions. Failure to do so could have disastrous safety and financial effects upon the IT systems and infrastructure, but more importantly the safety of employees.

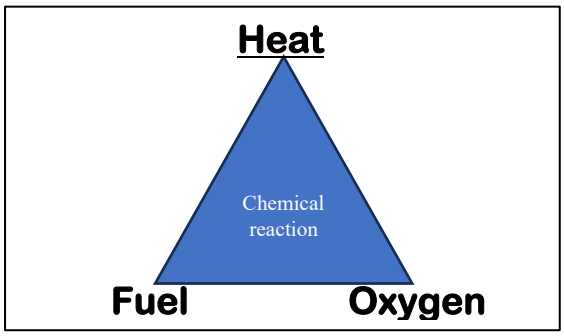
B. Liquids

Liquids pose a significant threat to a company's IT systems. Liquids can cause damage to electrical equipment through shorting electrical circuits, or through corrosion of electrical components.

One of the greatest risks that liquids can possess is the risk of flooding. In a peer reviewed article that evaluates various planning and assessment strategies for disaster preparedness, including physical security measures for critical systems like IT infrastructure, emphasising the need for comprehensive and integrated approaches to disaster management, Awah, L.S., Belle, J.A., Nyam, Y.S. et al. stated that hydrological damages and disasters accounted for 48.2% of all major damages and disasters globally in 2013. Although that is over a decade ago, they continued to report that the percentage has grown in the previous few decades and predict that it will continue to grow, particularly in coastal areas in the next 30 years due to climate change [10]. This article was published in 2024, therefore despite that data being from 2013, it is still incredibly relevant. This shows the massive danger that flooding can cause if it occurs around a data centre or an office. In addition to this, water can cause a risk on a smaller scale too, with just a small water leak being able to cause serious damage to electrical equipment. The risk could be prevented or mitigated using several physical security measures, which could include off-site cloud-based backup

storage in case of primary storage systems being lost, or integrating flood barriers and doors [11], [12]. On the other hand, having too little water can also be a problem too, as a water sprinkler system may be used as a last resort in the event of a fire. Having a lack of water would prevent this from being possible.

Liquids can pose non-flood related threats too in the form of chemicals. David Hutter wrote in 2016 that "the fire triangle consists of three elements, Heat, oxygen, and fuel. The chemical reaction located in the centre, represents what change occurs during fires". This can be seen in figure 1 below.



(Figure 1 – The fire triangle.)

The fuel, heat or chemical reaction mentioned can all be caused by poor security or control of chemicals. If, for example, a company that carried out lab work was unable to safely control their use of chemicals, there could be a fire or explosion caused, which could have drastic effects on a company's IT infrastructure if located close to. Hutter continues to write about how chemicals are used within gas discharge systems, that become active in the event of a fire. These gases include "carbon monoxide, halon, or halon substitutes". Failure to monitor the levels of chemical/gas reserves could cause a fire prevention system to become inactive, therefore reducing the physical security measures of a company's IT infrastructure in the event of a fire. This is a great source that, once again, shows both extremes of a source of risk for physical loss, by documenting the effects of unplanned chemical reactions and the risk of not having the correct chemicals to protect against other risks [13].

These useful sources clearly outline the risks of liquids to a company and their IT systems and infrastructure. Failure to control the liquids that may be present within their company will cause a lot of potential risk. To keep their IT systems safeguarded and secure, a company must be able to maintain stringent and robust control over both water and chemical risks.

C. Living Organisms

Living Organisms includes any living things that could pose any form of risk to an IT system. This could include viruses, bacteria, people, animals, insects etc.

The primary source of physical loss from living organisms is from people. This risk could emanate from within or outside of the company and could be accidental or with malicious intentions. Summarising the words of Philip P. Purpura, employees may steal from a company's IT infrastructure due to personal problems, such as financial problems which could be helped by stealing and selling sensitive data, or due to their environment, such as feeling alienated leading to wanting revenge on the company. External sources can also have similar motives but is generally viewed as more serious as it often comes in addition to gaining forced entry. Information tends to be stolen physically by smuggling the information out from its place of storage. The main countermeasures that Purpura documents are:

- Access Controls

These are used to "regulate people, vehicles, and items during movement into,

out of, and within a building or facility". Regulating access to certain areas ensures only authorised individuals can access sensitive information or prohibited areas. This could be achieved with methods such as ID tags, biometric scanning or CCTV & vehicle license plate recognition.

- Locks and keys

These are used to "hinder unauthorised entry" to a prohibited area. Ensuring that all windows and doors to prohibited areas are kept locked, only accessible with a physical key, prevents unauthorised access to both internal and external threats.

- Intrusion Detection Systems

These are used to "detect and report an event or stimulus within a detection area". This can be achieved using sensors, a control unit and an alarm system, which would then have to be responded to swiftly by a security member/team.

- Security Officers/Guards

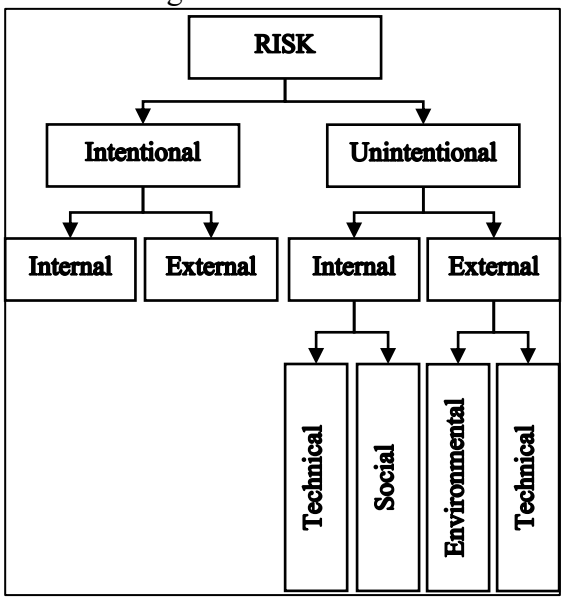
These are appointed security officials who oversee all security measures and checks within a company. This could include spot checks, patrols of the perimeter and tracking people entering and exiting site.

- Safes, Vaults and File Cabinets

These are protective containers that are used to secure valuable items. Physical items can be stored in these, only accessible with a key or code, with the added benefit of protection from fire, as well as protection from theft [14].

This is a fine source that covers many areas of physical security related to people, including motives, sources and methods of theft, which shows the level of thought and consideration a company must put into their IT security as there are so many different aspects and threats to consider, both internally and externally.

Another strong source for the topic of physical security against living organisms, particularly against people, is a source written by Ladislan Maris, Tomas Lovecek and Mike Zeegers. The source documents the methods for physical security with a link to differing natures of selected infrastructure systems. The source documents how risk can be broken down into several categories, which can be seen in figure 2 below.



(Figure 2 – Threat distribution diagram.)

The source continues to document that the "most common intentional external security risks include burglary, vandalism, sabotage, terrorist acts, industrial espionage, or any other offense affecting the entity's assets" and builds on this by outlining the different individuals, both internal and external, that could pose a threat to a company's IT infrastructure [15]. This is again another informative source which provides extensive lists of sources of risk, as well as clear explanation behind the reasoning for this risk.

D. Movement

Movement refers to the movement of the environment around an IT systems/infrastructure area. This could include collapse, shearing, shaking, vibration, liquefaction, flow waves, separation or sliding. Examples of movement could include "dropping or shaking of fragile equipment, earthquakes, mudslides, lava flows, sea waves, and adhesive failures" which shows how the biggest source of movement will come from natural events [3].

One source that documents the risk of movement to a company's IT infrastructure is written by Philip J. Ward et al. The source covers how natural hazards have led to over 1.6 million deaths in the past 3 decades and caused USD 260-310 billion worth of damage each year. The source also documents how, after recognising the necessity to mitigate these risks, there has been a significant advancement in global models for natural hazard risk assessments over the past decade. The paper continues to highlight the similarities and differences in approaches to assessing and mitigating different natural hazards, by reviewing various literature on the topic, using and comparing examples such as global risk studies on hydrological, climatological and meteorological hazards, as well as studies of earthquake and tsunami risk [16]. Again, this is a great article highlighting the importance of risk assessments and how different regions and sectors can learn from each other's risk reduction measures.

These previously highlighted sources show the catastrophic effects that a natural event can have upon a company's IT infrastructure. These catastrophic effects justify the need for protecting and safeguarding the IT systems. Another source, written by Sathurshan, Mathavanayakam et al. highlights the 4 R's of critical infrastructure resilience being robustness, redundancy, resourcefulness and rapidity, explaining why each is important with reasoning and examples behind each 'R' [17]. This source highlights exactly what a physical security measure, to protect against movement from natural events, must be. This can be used to determine the physical measures that must be used by a company to safeguard their IT infrastructure from movement. These measures would include elevated floors, earthquake-proof server racks, mag-locked doors, fire suppression systems, alarms and surveillance cameras. The risks to these systems can also be identified and responded to using risk assessments to analyse the risk of building an office/data centre in an area, as well as adequate recovery planning to react to any events that may occur [18].

III. Conclusion

Throughout this paper, the usefulness of various sources of literature has been reviewed to assess and qualify why modern organizations need to create an environment that protect, detect, react and safeguards applications using the organization's IT systems and infrastructure. In a world of advancing cybersecurity threats, it can be clearly seen why modern businesses must prioritise the protection of their IT systems and infrastructure in order to maintain a secure environment against these threats. This safe IT environment can be physically protected using the physical security measures which have been documented throughout this paper, which include controls, environmental monitoring, data backup, seismic retrofitting, flood barriers, and rigorous training. Implementing and

integrating these measures into a company will significantly enhance the resilience and robustness of its IT infrastructure. By addressing the most potent risks which include extreme temperatures, gases, liquids, living organisms, projectiles, movement and energy anomalies, a company can ensure the integrity and reliability of their IT systems, whilst also safeguarding against all types of threats.

Task 2

Contents

Task 2 7
1. Figures and tables 7
2. List of acronyms 7
3. Introduction 8
4. Organisation structure/chart 8
5. Policies and Procedures 10
6. Data Protection Compliance 10
7. Security Standards 11
8. Contingencies Planning 12
9. Governance and Strategic Planning for Security 13
10. Risk Management 14
11. Conclusion 15

References 15

1. Figures and tables

Figure 1 – An organisation chart showing the structure of the company

Figure 2 – A risk matrix to be used to plot the risks based on their likelihood and impact

2. List of acronyms

ISU – Information Security Unit

CISO – Chief Information Security Officer

AUP – Acceptable Use Policy

DPA – Data Protection Act

GDPR – General Data Protection Regulation

CMA – Computer Misuse Act

CSF – Cybersecurity Framework

NIST – National Institute of Standards and Technology

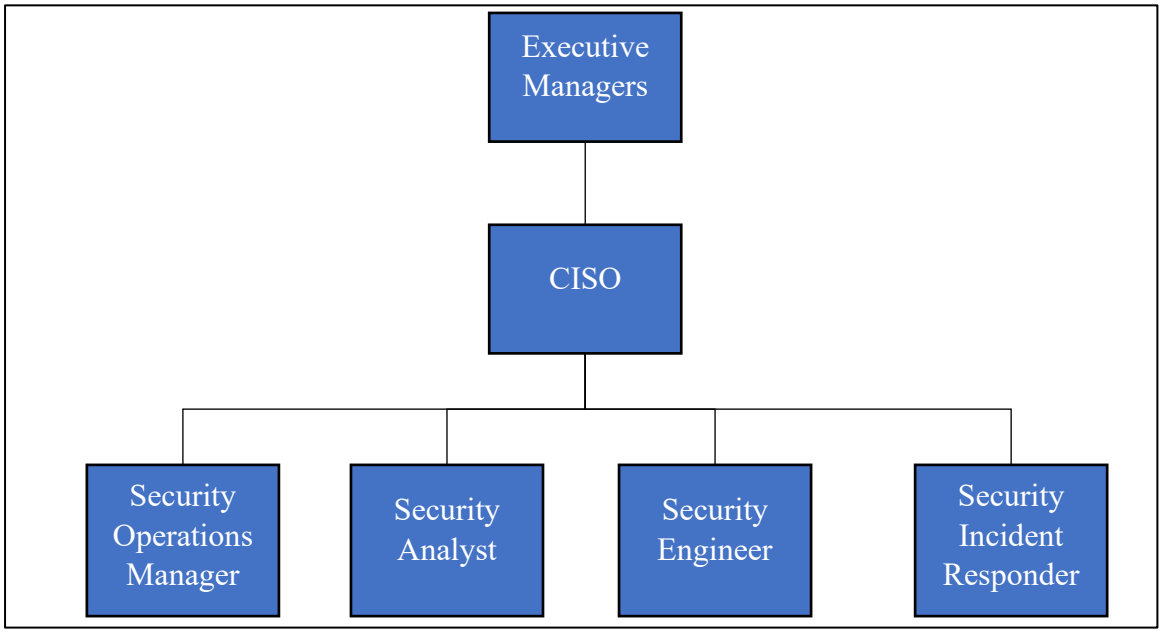
3. Introduction

For this case scenario, it will be assumed that the required new information security unit (ISU) will be for a small Financial Services company.

As a company, we must handle sensitive financial and personal data, and must meet several regulatory checks, therefore making information security critical to our operations as a business. The need for an ISU is of great importance as "cybersecurity is paramount for the financial services industry because it deals with vast amounts of sensitive financial and personal data. Protecting this data is essential to maintain trust, ensure regulatory compliance, and prevent financial losses" [19]. Therefore, the objectives of this new ISU are to be robust, to protect sensitive information and to comply with all data laws & regulations, in order to implement & maintain security standards, establish clear governance & accountability, and build customer trust & confidence, with the primary goal of protecting the business & it's profitability.

4. Organisation structure/chart

The structure of an organisation determines the roles & responsibilities, as well as the flow of information, within the organisation. Establishing a clear, well-defined structure is essential for clarifying these roles & responsibilities, and also allows for more effective communication between levels of the organisation. The organisation structure, which can be seen in the figure below, adopts a centralised structure as it allows for a well-defined chain of command and hierarchy [20].



(Figure 1 – An organisation chart showing the structure of the company)

The roles and responsibilities of each member within the organisation's ISU are:

- Chief Information Security Officer (CISO)

    - Roles:
        - Lead the ISU
        - Take charge of the overall strategy and execution of the program.
    - Responsibilities:
        - Develop security policies
        - Perform audits and risk assessments
        - Establish governance compliance plans
        - Supervise upon all other members within the structure
        - Report to executive management.
- Security Operations Manager
    - Roles:
        - Oversee daily operations within the team
    - Responsibilities:
        - Monitor security alerts
        - Manage data protection and access controls
- Security Analyst
    - Roles:
        - Gather intelligence regarding threats and attacks
    - Responsibilities:
        - Identify problems & threats
        - Monitor systems for vulnerabilities
        - Develop plans to prevent these threats
- Security Engineer
    - Roles:
        - Manage the overall security of the ISU infrastructure
    - Responsibilities:
        - Design & maintain highly secure network solutions
        - Implement firewalls to prevent cyber attacks
        - Ensure software development practices are up to date
- Security Incident Responder
    - Roles:
        - Lead the incident response strategy to mitigate damages from a cyber attack
    - Responsibilities:
        - Respond and mitigate security incidents
        - Coordinate the response team to resecure the company's data swiftly and efficiently [21], [22]

The proposed organisation structure will allow our company to have individuals with role-specific expertise focused on the essential areas of information security, ensuring that each area knows their roles, responsibilities and reporting lines, which will all contribute to the overall performance, efficiency and communication within the ISU.

5. Policies and Procedures

A policy is a course of action used by organisation to convey instructions from management to those who perform duties, and a procedure explains how to comply with a policy. IT policies and procedures "document how people and other IT systems can access your data and network. Policies and procedures work together with your technical security controls to protect confidential information from unauthorized access, disclosure, corruption, loss, and interference in both physical and electronic formats" [23].

The policies that I deem necessary, with justification as to why each policy is important, are:

- Acceptable Use Policy (AUP)

This policy defines what is acceptable and proper use of the company's technology asset, including information systems, resources, email, internet etc. This policy is important because it protects the company's assets & resources and increases productivity by reducing time spent on non-work-related activities.

- Data Protection and Privacy Policy

This policy defines our compliance as a business with data protection regulations, such as the GDPR, as well as specifying how sensitive data should be collected, processed and stored. This policy is important because it ensures we comply with the law, as well as demonstrates to our customers that we prioritise security and that their sensitive data is safe with us, which will give them far more confidence in our company.

- Data Access Control Policy

This policy defines how data is classified, depending on its type and sensitivity, allowing access according to an individual's job role/authority. This policy is important as it ensures the confidentiality, integrity and availability of sensitive data is maintained throughout business, using various methods of restrictions and permissions, again demonstrating our prioritisation of security to our customers.

- Remote Access Policy

This policy defines how an employee, as well as third parties, are allowed to connect to the company's IT systems. This policy is important as it allows our cybersecurity to be maintained whether our employees are working in the office or remotely, by clearly documenting the permissions and protocols for anyone accessing the company's network.

- Incident Response Policy

This policy defines the procedures for identifying and responding to a potential security threat, which includes guidelines for communication and incident documentation. This policy is important because it ensures that there is a clear plan in case of an incident, therefore minimising the risk and the impact of a potential incident [23], [24], [25].

6. Data Protection Compliance

As previously stated, as a finance company with a huge amount of sensitive data, we must adhere to several laws and regulations to ensure we are adequately safeguarding this data.

Failure to comply with these stringent rules and regulations will result in our company being able to mitigate risks, avoid legal penalties or to maintain a strong reputation within the industry. The main data protection laws and regulations that we must comply to are:

- Data Protection Act 2018 (DPA)

As of the UK leaving the European Union, the Data Protection Act of 1998 was updated to reflect the new laws and regulations and is now "the UK's implementation of the General Data Protection Regulation (GDPR)". The DPA "controls how your personal information is used by organisations, businesses or the government". The DPA requires that all personal data is:

  - used fairly, lawfully and transparently
  - used for specified, explicit purposes
  - used in a way that is adequate, relevant and limited to only what is necessary
  - accurate and, where necessary, kept up to date
  - kept for no longer than is necessary
  - handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage [26].

We must comply with this law to ensure that we convey a professional and trustworthy image to our customers, so that they feel confident to use our services. We must also comply as, ultimately, it is a fundamental law protected and enforced by the law.

- Computer Misuse Act 1990 (CMA)

The CMA is a law that "criminalises several acts, including accessing data without authorisation and installing malware on a person's computer". These criminalised acts include unauthorised access to computer material with intent to commit a crime, with intent to impair the use of the computer or with the intent to cause serious damage or harm, or the "development, distribution, or obtaining of malware, password crackers" [27]. We must comply with these laws and ensure that nothing like this is being done by our employees, as failure to comply can result in penalties including imprisonment and fines for anyone involved.

We will ensure that these laws are complied with by integrating them into our policies & procedures, ensuring that every employee is aware of the rules and regulations they must follow, and by performing regular audits to ensure our compliance standards are up to date.

7. Security Standards

Security Standards are "a document written by subject experts which distils and codifies best practice" [28]. These standards are a framework and are used to check and ensure that they're performing in the best way possible, according to the standards. These standards, just like the policies & procedures and rules & regulations mentioned above, will help us to maintain integrity and confidentiality of all of our sensitive data we possess as a company, ensuring we'll be meeting all regulatory requirements. In addition, a lot of these standards focus on risk management and regulatory compliance, so that is another great benefit of achieving them, whilst also contributing to our overall operational efficiency.

The security standards I believe we should adopt are:

- ISO/IEC 27001

ISO/IEC 27001 is an international standard for Information Security management and is "the ultimate benchmark for businesses to establish, implement, operate, monitor, review, maintain, and continually improve an information security management system". Achieving this standard will lead to our company having improved information security, advanced strategies, continuous improvement throughout the company, and greater trust from our customers. ISO/IEC 27001 certification can be achieved by auditing our existing procedures and working with ISO consultants to improve upon them and create a manual documentation, setting out how business operations should be performed moving forward. Certification is finally provided by an auditor once they've confirmed that we are conforming to the standards. [29].

- ISO/IEC 17799

ISO/IEC 17799 is a framework for information security that "establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization" focussing on the best practices of control in Information Security management areas such as security policy, asset management, HR security, physical & environmental security, communications & operations management, access control, business continuity management, etc. Overall, the framework shows that organisational security policy is needed for management direction and support. [30]

- NIST Cybersecurity Framework (CSF)

This framework developed by the National Institute of Standards and Technology (NIST) helps to improve the cybersecurity of a company's critical infrastructure. The CSF "provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks". The CSF consists of 3 components:

  - CSF Core which is "a taxonomy of high-level cybersecurity
  - outcomes that can help any organization manage its cybersecurity risks. The CSF Core components are a hierarchy of Functions, Categories, and Subcategories that detail each outcome".
  - CSF Organisational Profiles which are "a mechanism for describing an organization's current and/or target cybersecurity posture in terms of the CSF Core's outcomes".
  - CSF Tiers which "can be applied to CSF Organizational Profiles to characterize the rigor of an organization's cybersecurity risk governance and management practices" [31].

These standards must, once again, be implemented via structured policies & procedures and regular audits, which will provide us with a robust security environment which supports our business and protects our assets.

8. Contingencies Planning

A contingency plan is a strategy that is designed to be used by a business to respond to and mitigate any negative unforeseen events that may occur in the future. In our business' case, a negative event could be a cyber-attack, natural disaster or a systems failure. Having a proactive

approach will help protect critical assets, maintain customer trust, and support long-term business success. The contingency planning process involves the following steps:

- Develop a Contingency Plan policy statement

This step is about creating a policy which outlines the need for a contingency plan and describes the scope, purpose and objectives of the plan.

- Conduct Business impact analysis

This step is about researching the adverse events that could impact our business, and how each possible event could affect critical business processes and operations.

- Identify preventive controls

This step is about the measures which we can put in place to reduce the likelihood of disruptions and mitigate their impact on our company. This step would involve performing risk assessments, evaluating potential controls and then implementing them where they're required.

- Create contingency strategies

This step is about the plan of action in the instance that a negative event has taken place. It is a strategy for maintaining as much functional operation as possible and recovering from a disruption quickly and effectively. This step could include strategies such as data backup & recovery, alternative working arrangements or redundant/duplicate servers, power supplies etc.

- Develop contingency plan

This step is about creating the actual documentation for the plan, so that all necessary information, procedures and outcomes for the planned strategies in case of an emergency is clearly documented.

- Ensure plan testing, training, and exercises

This step is about the regular testing, training and exercises of the contingency plan's procedures and strategies, so that all employees and personnel are adequately prepared to carry out the documented steps. This step could be done with a series of drills, simulations, courses and e-learning modules.

- Ensure plan maintenance

This step is about maintaining the contingency plan in order to keep it relevant, up to date and therefore effective at all times. Failure to do so can result in certain step becoming out-dated and obsolete and therefore useless. The contingency plan must be monitored and reviewed consistently with a series of audits and assessments, allowing us to adapt and improve the contingency plan documentation based on the feedback provided.

9. Governance and Strategic Planning for Security

Information Security Governance is a set of responsibilities and practices exercised by our company's board and executive management. The goal of Governance is to provide strategic direction, establishment of objectives , and measurement of progress toward objectives.

Information Security Governance has 5 main goals which include Strategic alignment, Risk management, Resource management, Performance measurement and Value delivery. We must integrate a governance system into our business, which complies to ISO/IEC 38500 which is "the international standard for the corporate governance of information technology, and provides guidance to those advising, informing or assisting directors on the effective and acceptable use of information technology within the organisation" [32]. Strategic planning provides a clear strategy for implementing and maintaining security measures. This must be done by establishing a governance framework, developing a strategic security plan including a vision and objectives, and finally seamlessly integrating it into the business' strategy.

10. Risk Management

Finally, the last crucial component of my proposed ISU is risk management, which is "the systematic process of identifying, assessing, and mitigating threats or uncertainties that can affect your organization. It involves analysing risks' likelihood and impact, developing strategies to minimize harm, and monitoring measures' effectiveness" [33]. I propose that our risk assessment procedure adopts the following method:

- Identify hazards

This is determining the potential sources of risk within our company that could have an adverse effect on our assets or operations.

- Assess risks

We must assess the likelihood and the impact of a hazard occurring and applying quantitative and qualitative measures to each, which can then be plotted in a risk matrix (seen in figure 2 below) to help visualise the high-priority risks.

		Impact				
Likelihood		Negligible	Minor	Moderate	Significant	Severe
	Very likely	Low Med	Medium	Med High	High	High
	Likely	Low	Low Med	Medium	Med High	High
	Possible	Low	Low Med	Medium	Med High	Med High
	Unlikely	Low	Low Med	Low Med	Medium	Med High
	Very unlikely	Low	Low	Low Med	Medium	Medium

(Figure 2 – A risk matrix to be used to plot the risks based on their likelihood and impact)

- Control risks

This is implementing the measures to mitigate or eliminate the previously identified risks. This could include extra firewalls, employee training or regular system updates.

- Record findings

We must ensure that the entire process is documented for transparency, justification of any changed made and for future reviews.

- Review controls

We must review the controls to ensure they are consistently effective and relevant to mitigating risk. Again, this would be done using audits, systems updates and management reviews [34].

11. Conclusion

In conclusion, establishing a new robust ISU in our company is of critical importance to protect our sensitive information, to comply with regulations and to build trust within our customers. By following the structured approach that I have outlined in this report, I believe we will be covering all areas of information security and will be building a resilient system which will lead us, as a company, to long-term success in the future.

References

[1] "The CSF 1.1 Five Functions," NIST, 26 02 2024. [Online]. Available: https://www.nist.gov/cyberframework/getting-started/online-learning/five-functions. [Accessed 25 07 2024].

[2] A. Mahn, "Identify, Protect, Detect, Respond and Recover: The NIST Cybersecurity Framework," NIST, 23 10 2018. [Online]. Available: https://www.nist.gov/blogs/taking-measure/identify-protect-detect-respond-and-recover-nist-cybersecurity-framework. [Accessed 25 07 2024].

[3] "Physical (Environmental) Security," Flylib, [Online]. Available: https://flylib.com/books/en/1.564.1/physical_environmental_security.html. [Accessed 25 07 2024].

[4] D. B. Parker, Fighting Computer Crime, Wiley, 1998.

[5] J. Andress, The Basics of Information Security, 2014.

[6] "Why Fires Are Such a Threat to Data Centers and Computer Equipment," Ceasefire, 09 06 2022. [Online]. Available: https://ceasefire.com/firesuppression/article/why-fires-are-such-a-threat-to-data-centers-and-computer-equipment. [Accessed 26 07 2024].

[7] "PHYSICAL SECURITY & FIRE SUPPRESSION | KEEPING DATA SAFE," Cyberfort Group, [Online]. Available: https://cyberfortgroup.com/colocation/physical-security-fire-suppression-keeping-data-safe/#:~:text=Many%20data%20centres%20rely%20on,actually%20turn%20into%20a%20fire.. [Accessed 26 07 2024].

[8] "Extreme Cold," CISA, [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/extreme-weather-and-climate-change/extreme-cold. [Accessed 26 07 2024].

[9] E. Anderson, "Chilling Cyber Security Threats," Converged, 17 01 2024. [Online]. Available: https://converged.co.uk/chilling-cyber-security-threats/#:~:text=Snow%20and%20freezing%20temperatures%20impact%20physical%20security&text=To%20address%20these%20physical%20security,of%20redundancy%20for%20critical%20components.. [Accessed 26 07 2024].

[10] L. S. Awah, J. A. Belle, Y. S. Nyam and I. R. Orimoloye, "A Systematic Analysis of Systems Approach and Flood Risk," 2024.

[11] "How to Stay Safe when Flooding Occurs," The Flood Hub, 16 11 2023. [Online]. Available: https://thefloodhub.co.uk/blog/how-to-stay-safe-when-flooding-occurs/#:~:text=Properly%20installing%20Property%20Flood%20Resilience,your%20property%20from%20flood%20damage.. [Accessed 07 28 2024].

[12] J. Careless, "How to maintain a solid cybersecurity posture during a natural disaster," CSO, 30 11 2023. [Online]. Available: https://www.csoonline.com/article/1249508/how-to-maintain-a-solid-cybersecurity-posture-during-a-natural-disaster.html. [Accessed 28 07 2024].

[13] D. Hutter, "Physical Security And Why It Is Important," pp. 24-26, 2016.

[14] L. J. Fennelly and P. P. Purpura, "Effective Physical Security," ProQuest Ebook Central, 2016, pp. 181-248.

[15] L. Maris, T. Lovecek and M. Zeegers, "Security of Infrastructure Systems: Infrastructure Security Assessment," *Safety and Security Issues in Technical Infrastructures,* pp. 353-382, 2020.

[16] P. J. e. a. Ward, "Natural hazard risk assessments at the global scale," vol. 20, no. 4, 2020.

[17] M. e. a. Sathurshan, "Resilience of Critical Infrastructure Systems: A Systematic Literature Review of Measurement Frameworks," 2022.

[17] "The Importance of Physical Security," AGIO, [Online]. Available: https://agio.com/the-importance-of-physical-security/#gref. [Accessed 29 07 2024].

[18] S. Bowcut, "Securing financial services: A focus on cybersecurity," Cybersecurity guide, 06 12 2023. [Online]. Available: https://cybersecurityguide.org/industries/financial/. [Accessed 16 07 2024].

[19] W. Kenton, "Organizational Structure for Companies With Examples and Benefits," Investopedia, 22 06 2024. [Online]. Available: https://www.investopedia.com/terms/o/organizational-structure.asp. [Accessed 16 07 2024].

[20] "Cyber Security Team Structure: Roles & Responsibilities," Nordic Defender, 19 12 2022. [Online]. Available: https://nordicdefender.com/blog/cyber-security-team-structure. [Accessed 07 16 2024].

[21] "Understanding Cyber Security Team Roles and Responsibilities," Tufin, 12 10 2023. [Online]. Available: https://www.tufin.com/blog/understanding-cyber-security-team-roles-and-responsibilities#:~:text=However%2C%20a%20typical%20cybersecurity%20team%20includes%20the%20following,Responder%3A%20Specializes%20in%20handling%20and%20mitigating%20security%20inciden. [Accessed 16 07 2024].

[22] M. Sloss, "Why Are IT Policies & Procedures Important," Bellwether, 15 10 2019. [Online]. Available: https://www.belltec.com/2019/03/it-policies-procedures/. [Accessed 16 07 2024].

[23] "ISO 27001 Policies Ultimate Guide," HighTable, [Online]. Available: https://hightable.io/iso-27001-policies/. [Accessed 16 07 2024].

[24] K. Bowman and J. Tunks, "Understanding Data Access Control: A Comprehensive Guide," Pathlock, 08 04 2024. [Online]. Available: https://pathlock.com/learn/data-access-control/#:~:text=Data%20access%20control%20is%20a%20protective%20strategy%20that,availability%20of%20sensitive%20information%20through%20restrictions%20and%20permissions.. [Accessed 23 07 2024].

[25] "Data protection," GOV.UK, [Online]. Available: https://www.gov.uk/data-protection. [Accessed 23 07 2024].

[26] R. Bateman, “Computer Misuse Act 1990,” Terms Feed, 12 05 2024. [Online]. Available: https://www.termsfeed.com/blog/computer-misuse-act-1990/#About_The_Computer_Misuse_Act_1990. [Accessed 23 07 2024].

[27] “Why standards are so important to security professionals,” City Security, 31 07 2018. [Online]. Available: https://citysecuritymagazine.com/risk-management/security-standards/#:~:text=These%20standards%20%E2%80%93%20written%20with%20the%20help%20of,security%20products%2C%20security%20management%20systems%20and%20security%20services.. [Accessed 23 07 2024].

[28] “ISO/IEC 27001,” IMSM, [Online]. Available: https://www.imsm.com/us/iso-27001/?keyword=cyber%20security%20standards&matchtype=e&network=o&device=c&utm_term=cyber%20security%20standards&utm_campaign=LOL%20-%20Search%20-%20UK%2027001%20&utm_source=bing&utm_medium=cpc&hsa_acc=140168856&hsa_cam=3766454. [Accessed 23 07 2024].

[29] “ISO/IEC Standard 17799,” enisa, [Online]. Available: https://www.enisa.europa.eu/topics/risk-management/current-risk/laws-regulation/rm-ra-standards/iso-iec-standard-17799. [Accessed 23 07 2024].

[30] NIST, “The NIST Cybersecurity,” NIST, 26 02 2024. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 23 07 2024].

[31] “ISO/IEC 38500,” it governance, [Online]. Available: https://www.itgovernance.co.uk/iso38500. [Accessed 23 07 2024].

[32] K. Gibson, “WHAT IS RISK MANAGEMENT & WHY IS IT IMPORTANT?,” Harvard Business School Online, 24 10 2023. [Online]. Available: https://online.hbs.edu/blog/post/risk-management. [Accessed 23 07 2024].

[33] “Managing risks and risk assessment at work,” Health and Safety Executive, [Online]. Available: https://www.hse.gov.uk/simple-health-safety/risk/steps-needed-to-manage-risk.htm. [Accessed 24 07 2024].