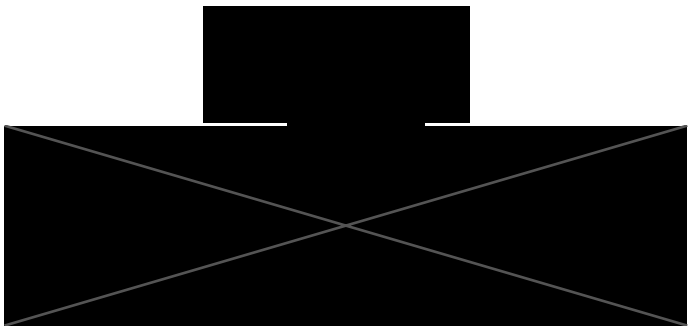

Information Security Management risk assessment of a design company based in the UK

Niccolò Barbini

Contents

List of Tables

List of Figures

Chapter 1

Introduction

During the past centuries, business activities have changed their way of protecting their core information from being stolen by competitors or criminals (Amara, Landry, and Traoré, 2008). The digital revolution has brought considerable advantages in two principal areas: how business operations are conducted and how business assets are protected (Pousttchi, Gleiss, Buzzi, and Kohlhagen, 2019). Despite representing a considerable improvement in business activities, the digital revolution brought a lot of drawbacks with itself; these drawbacks could be:

- Information Protection
- Human risks
- Stealing of data (e.g., customer, company, suppliers)
- Cyber and Physical infrastructure attacks

However, some solutions can increase the company's awareness related to these areas; from risk assessment and pen-testing to risk information security management, these solutions aim to improve the chance for a business to identify its vulnerable points and deploy solutions to contrast them. In this document, an information security management assessment has been conducted to help a design company to analyse its structure and resilience against these modern threats; the goal of an information security management assessment is to ensure the protection of confidentiality, availability, and integrity of assets from threats and vulnerabilities (Blakley, McDermott, and Geer, 2001). Not protecting these areas could represent a substantial negative influence on the company's finances, a negative influence on reputation, a slow-down decision-taking mechanism, or the discontinuance of business operations (Sardjono and Cholik, 2018).

1.1 Purpose

This information security management assessment aims to evaluate the cyber and physical security of the company called ABCD. The author interviewed the IT manager on the [redacted] through the Microsoft Teams software. After the interview, which lasted 45 minutes, the author has analysed in detail the following nine areas from a cyber and physical security perspective:

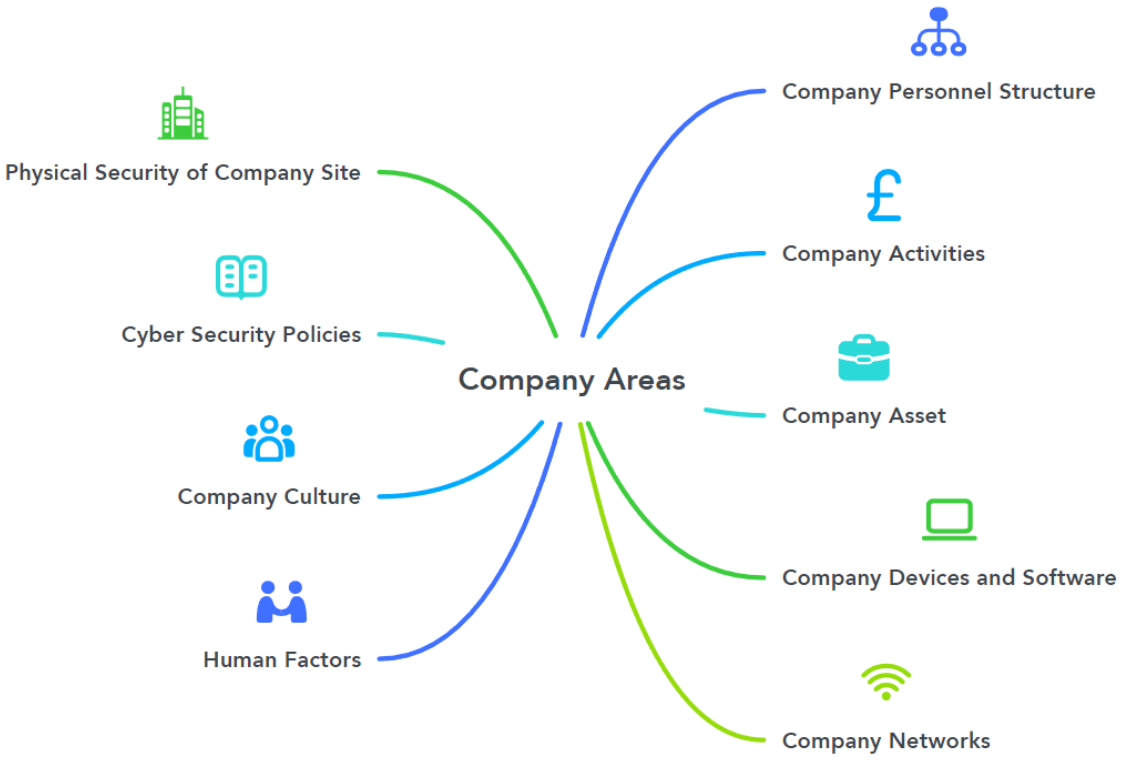

Figure 1.1: Company Areas Representation

In the following chapters of this report, the author examines the areas presented in figure 1.1; thus, the necessary suggestions to anticipate, mitigate and enrich the current security measures are suggested.

Chapter 2

Company Activities, Structure and Assets

In this chapter, the author illustrates the company's areas.

2.1 Company Activities

The core business activity of the company ABCD is to design and sell tailored lightning and lightning scheme for:

- Private Houses
- Restaurants
- Boutiques
- Hotels

Despite designing lighting control systems and supplying light fittings, the company does not install electrical systems.

2.2 Company Structure

Currently, the company has eight employees in total. One is the IT manager/ business owner, the other is the financial manager, and the remaining six are employees. In the future, there will be the possibility to employ ten people.

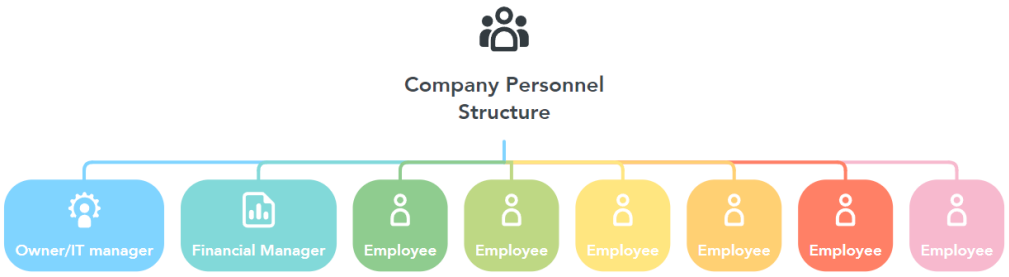

Figure 2.1: Company Personnel Structure Representation

2.3 Company Security Role

In this company, the IT manager is the person responsible for cyber security. Briefly, the IT manager, who has worked over twenty years in the IT sector, has the following skills:

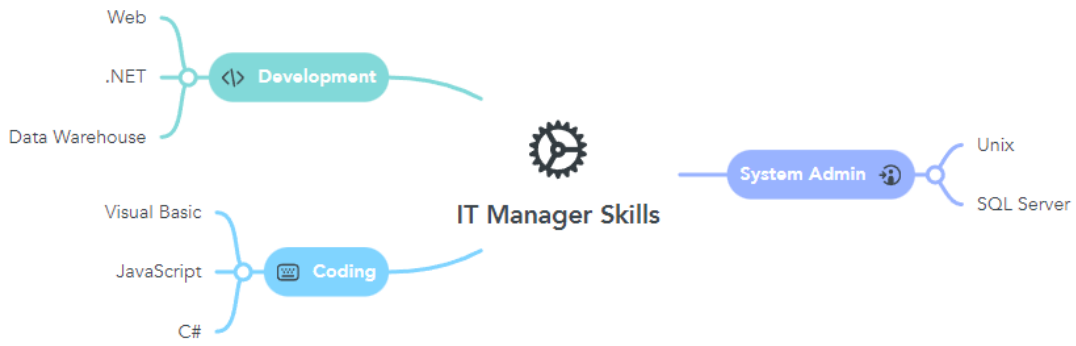

Figure 2.2: IT Manager Skills

2.4 Company Assets

According to ABCD's spokesperson, the company does not have many assets. Despite having physical tools, devices and hardware, the company's most precious assets are its employees' knowledge and skills. Below, the assets list is presented:

- PC laptop and Desktop computers
- Leasing machines
- Knowledge and skills from the designers
- Company facilities (the buildings are used with a long-term leasing contract)

Regarding Intellectual property (IP), the company declared that what they own is the rights and copyright of the designs where the client or clients owned the design. Consequently, ABCD stated that the rights and copyrights are their intellectual property.

Chapter 3

Company Cyber Culture and Public Relation

In this chapter, the company working, security culture and public relations are examined.

3.1 Cyber and Computing Culture

Considering the number of the company's employees, there is a familiar working culture where people tend to help each other; for example, with cyber issues. Given that human errors can occur, there is no tendency to blame employees. An example of this culture was shown years ago when one of the employees fell victim to a phishing mail attack, and colleagues tried to help rather than blame this person. Moreover, this episode helped people to acknowledge the chance of facing online risks, and they have developed a practical measure to contrast this phenomenon by sharing screenshots of suspected emails.

3.2 Company Policies, Standards and Insurance

The company uses classic-old policies to regulate the cyber security rules and actions to contrast, anticipate and mitigate cyber security issues. Also, employees know that the IT manager can access, check, and control their online and offline activities from work devices. The company does not disclose details about its security policy.

3.3 Public relation

For a business that operates with the public, it is vital to keep a relationship with the media and have a quick plan when a cyber-attack hits the company and damages it (González-Herrero and Smith, 2008). In ABCD, the responsibilities and roles are clear; for example, the IT manager deals with the Information Commissioners Office (ICO). Despite adopting the EU General Data Protection Regulation (GDPR) (Tankard, 2016), the company does not have a data protection officer because its administrative structure allows it to do that.

Chapter 4

Company Relation with Suppliers

This chapter analyses the relationship between the company and suppliers.

4.1 Suppliers

The company does not share projects or at least a tiny part of a client project with the manufacturers/suppliers. It shares the following information:

- Product supply
- Pricing (which is made entirely by the company through an internal process)
- Deliveries
- Products development

During the interview, the company speaker highlighted that the measures adopted by the company are not from a security perspective but from a frequent practice in the industry.

Chapter 5

Hardware, Software, Network and Building representation

In this chapter, the company devices and network are described alongside a representation of the office's site.

5.1 Work and Software Devices Description

In this section, work devices are listed; a view of the company's devices is vital to understand the risks.

Work Devices

The company owns the following devices:

- Windows Desktop and Laptops
- Linux Development box

Work Software

The company uses the following software:

- Microsoft 10 Professional as Operative System (OS)
- Office 365
- Dropbox
- Microsoft Azure
- Google Chrome
- High Rise (Customer Relationship Management (CRM) system)
- Sage (Financial Information Software)
- Bitdefender (Antivirus service for desktop and laptop pc)

Considering the importance of costs, the software used by ABCD is a workable solution for a business of this size.

5.2 Company Network and Guest Access

The company has an internal network that connects devices through wired and wireless connections. For example, desktop PCs are connected via Ethernet cable while laptops are via internal WI-FI. The connections are high-speed thanks to the fibre connection and a copper connection; also, a package router helps to transport and receive internet packages. A firewall and WPA2 wireless connection are used to enforce the network's security. An external ADSL modem is used to create a different network for guests.

5.3 Company Building representation

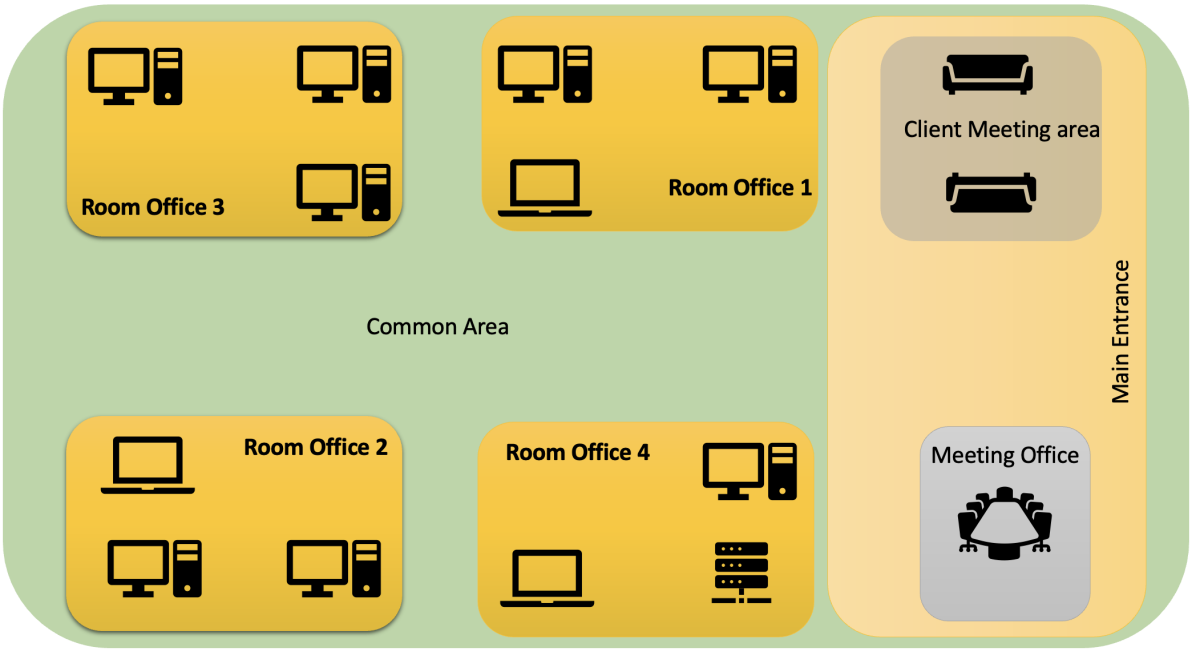

Figure 5.1: Company Building Representation

Chapter 6

Company Solution for facing Cyber Attacks

After trying, different services to share work updates for a while, the company decided to use e-mail for internal communication between employees. Also, the software for online storage, called Dropbox, is vastly used internally to share updates and new features on different works. Furthermore, Quotewerks software is used to manage product project specifications. Regarding external communications, email service and the software Microsoft Teams are used.

6.1 Standard procedure

Whether a cyber-attack is successful or not, an attack assessment is performed to understand the identity and damages provoked by the attack. Meanwhile, the company uses two software to guarantee that data are not lost and that daily activities can run without many issues caused by cyber-attacks; these two software are:

1. Dropbox
2. Microsoft Azure

Considering the resilience and efficiency of the two software, the IT manager is confident of getting back up and running after an attack (e.g., ransomware) despite the risk and damages that this attack cause.

6.1.1 Dropbox

Dropbox performs data backups and allows to roll company's files back to thirty days. They evaluated this procedure and its efficiency by destroying chunks of data and restoring them. The outcome of this test has been successful, and it is possible to recover and restore most of the company's data; it is essential to bear in mind that this software allows restoring data in 30 days' time and the ability of Dropbox to rewind folders is not suitable for the company, according to ABCD's spokesperson.

6.1.2 Microsoft Azure

Microsoft Azure is used for storing and backing up data; its backups up automatically two times a day. Regarding the warehouse, the system saves files eight times a day.

Chapter 7

Critique of the Company areas

In this section, the author evaluates the company's structure, resilience, and security. At first look, the company areas have good cyber resilience against cyber-attacks. Despite presenting a good structure, the author has made suggestions to increase security and resilience against cyber-attacks. Thus, it has been possible to identify two significant areas that require improvement in terms of security; they are:

- Human areas
- Physical security

7.1 Advantages and Disadvantages of Company structure

It has been possible to state the disadvantages and advantages of the structure considering the elements described in the previous chapters.

Advantages

The advantages of the current company status are:

- Great choices of software and habits to updating them to the most recent working version
- Great company culture, both for human relationships and for cyber security prevention measures
- Company roles are well defined
- Great cyber hygiene/practices to increase security and resilience

Disadvantages

Alongside the advantages, it has been possible to identify certain disadvantages, which are:

- Too much trust in the Employees
- Policies are outdated

7.2 Physical Security Measure

After the evaluation of the physical security measures of the company, it has been possible to state that some improvements could be beneficial to increase the level of security. The first measure to adopt is to disable USB ports of company devices because they represent a considerable vulnerability from a cyber perspective and a physical one since it is possible to conduct attacks from this source (Nissim, Yahalom, and Elovici, 2017). This measure should not be of great distress for the company employees, considering that most software they use for their work activities are synchronised with cloud services. The second measure to adopt is to install a control system which allows only specific people to enter certain company facility areas; a radio frequency identification technology (RFID) system could be a congenial idea considering the cost and benefit of this technology (Weis, 2007). Using these two measures, physical security can improve drastically.

Chapter 8

Evaluation of Company Information Security Management

In order to perform a deep and detailed Information Security Management Risk assessment, it is essential to visualise the four main steps necessary to perform this study (Nyanchama, 2005). They are:

1. Identify Risks
2. Evaluate Risks (Analysis, Strategy, Policies)
3. Threat Risks (Anticipation, Treatment, Mitigation, Avoidance and Acceptance)
4. Handle Changes

8.0.1 Identify Risks

In this step, different factors or sources of risks have been found and explained briefly.

- Vulnerabilities: Weakness present in the company facility, technologies, people and relationship
- Threats: Players (insiders or outsiders) that might generate incidents if they exploit one of the vulnerabilities
- Assets: They are valuable information content such as PCs, Routers, Company property
- Impacts: They are defined as the harmful effects or consequences of incidents and calamities which affect the assets, damaging the company and its business interest

8.0.2 Evaluate Risks

This stage involves examining all the information collected during step 1 to determine the grade of different risks. Evaluate risks stage is vital in this process considering the flexibility for risks that, in general, companies take; moreover, the strategies and policies selected and followed by the company are strictly related to cultural drivers and personal attitudes of people involved in risk management activities (Anwar et al., 2017).

8.0.3 Threat Risks

This stage drives the necessary actions for mitigating, anticipating, sharing, and accepting risks.

8.0.4 Handle Changes

Despite appearing obvious, it is crucial to remember that changes are handled as one of the most important actions to follow. That is because the information security sector is dynamic, and a pivotal point to succeed in this area is to study and update the way of answering the risk (Zheng, Li, Xu, and Zhao, 2022). This is the reason why the measure against risks should be bespoken, not standardised.

8.1 Frameworks Presentation

Before reaching a conclusion about which risk framework suits better the necessity of the company examined in this report, the author has made a comparison between a group of well-known frameworks used in the industry; the risks framework analysed by the author are:

- ISO 27K family
- Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) Allegro
- Failure Mode And Effect Analysis (FMEA)

Despite its utilisation worldwide, the ISO 2K (Everett, 2011) family does not represent an ideal choice for our purpose, considering it is unsuitable for a small organisation. Consequently, the author examined two other models: OCTAVE Allegro and FMEA.

8.2 Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE ALLEGRO)

OCTAVE is a suite of tools, techniques and methods for the assessment and planning of risk-based information systems security (Sardjono and Cholik, 2018); the OCTAVE method consists of three phases that are required by the OCTAVE criteria (Albert and Dorofee, 2001) (Gutandjala, Gui, Maryam, and Mariani, 2019). Currently, there exist three different OCTAVE models: (Sardjono and Cholik, 2018)

- OCTAVE
- OCTAVE-S
- OCTAVE Allegro

In this report, the author decided to utilise the OCTAVE Allegro model, which focuses on information assets and data that support that information. The reason behind this choice is that this method focuses on information assets regarding their use, where they are saved, and how they are moved and treated, considering their threats exposition, vulnerabilities, and the result of the disruption (Caralli, Stevens, Young, and Wilson, 2007). OCTAVE Allegro is made of four steps which contain eight sub-steps; they are:

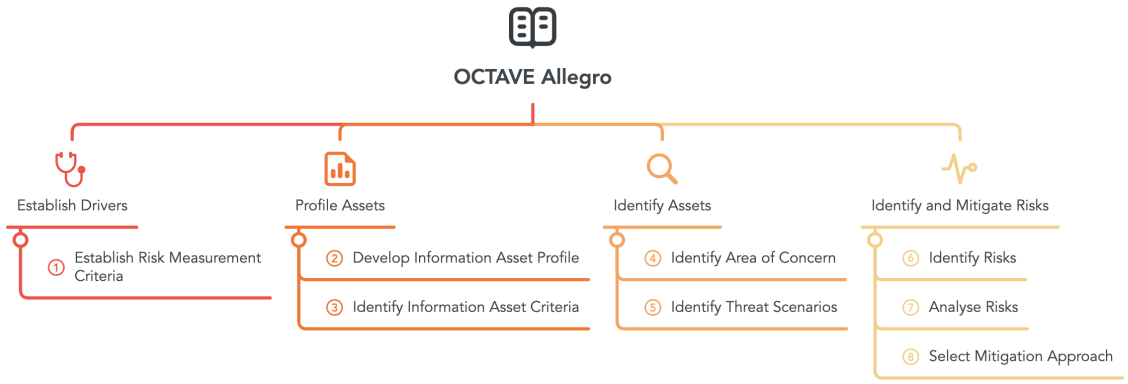

Figure 8.1: OCTAVE Allegro model - inspired by (Gutandjala, Gui, Maryam, and Mariani, 2019)

8.3 Failure Mode And Effect Analysis (FMEA)

FMEA is an ordinary process analysis tool; its purpose is to take measures to remove or minimise failures, beginning with the highest-priority one (ASQ, 2005). The selection of these failures is based on how severe their consequences are, how often they happen and how effortlessly they are discovered; these steps are necessary for a dynamic system that continuously allows continuous improvement. The decision to use FMEA has been made by its characteristics of being used to analyse the threats and vulnerabilities within the company (Schmittner, Gruber, Puschner, and Schoitsch, 2014).

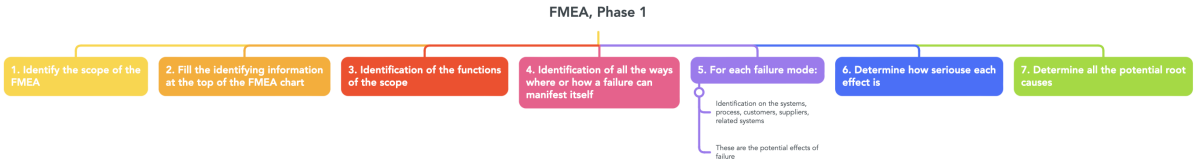

Figure 8.2: FMEA procedures for threats and vulnerabilities Phase 1 - inspired by (ASQ, 2005)

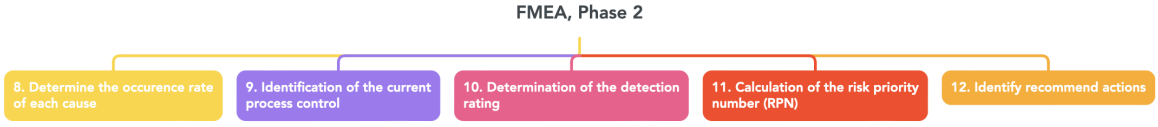

Figure 8.3: FMEA procedures for threats and vulnerabilities Phase 2 - inspired by (ASQ, 2005)

In the next section, the author describes the reason behind the decision to utilise a hybrid framework composed of OCTAVE Allegro and FMEA.

Chapter 9

OCTAVE Allegro and FMEA Standards

After a detailed analysis, it has been possible to evaluate the company and explain the potential vulnerabilities and threats which ABCD can face. Despite identifying nine company areas (see Chapter 1, section 1.1), four principal areas have been studied due to their vital relevance for risk assessment. A first analysis of the areas has been conducted with OCTAVE Allegro, while a deep examination of threats and vulnerabilities has been done with FMEA.

9.1 OCTAVE Allegro

In this section, the author uses OCTAVE Allegro; as the first step of this process, it is crucial to establish risk measurement criteria. They are reported in Appendix A (sections A.1 and A.2). Once this phase is concluded, it is possible to start the profile assets section. To identify the profile assets, the author tried to identify the critical information asset profile for ABCD; the following criteria used in this step are reported:

- Information Asset regarding Human Factors (Customers Trust, Employees)
- Information Asset concerning Policies
- Information Asset relating to Suppliers
- Information Asset regarding Devices and Software
- Information Asset concerning Network

In Appendix A (section A.3), the author illustrates the critical assets identified within a table. Once the areas of concerns, assets and motivations regarding their choices have been identified, the following steps are to rank their impacts and assign them a score. The score is essential since it is an indicator of the mitigation order of the asset risks.

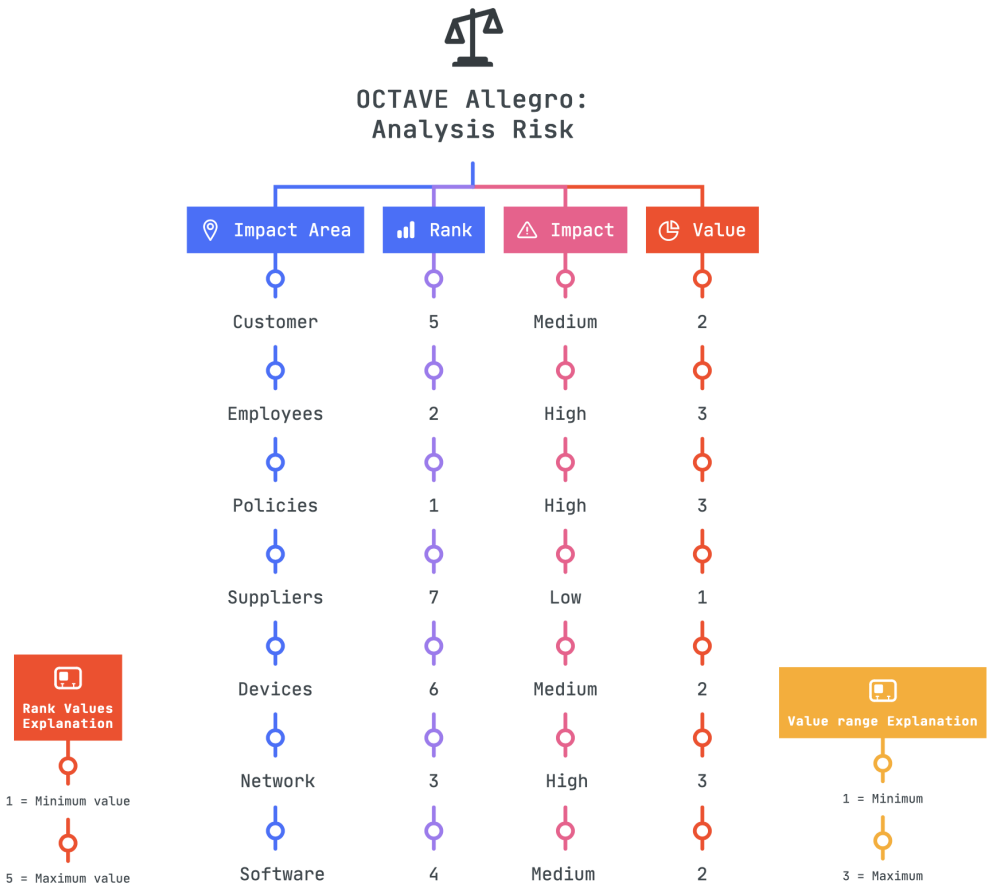

Figure 9.1: Ranking of impacts

As the figure 9.1 suggests, the top three concerns for ABCD are employees, policies, and networks. The Customer section is considered subject to risks; for example, a breach in this area can damage the company, but the consequences associated with this area are not comparable with the consequences associated with a policy not followed or, even worse, the company network cannot operate; consequently, it has received a medium impact score.

9.2 FMEA

FMEA framework has been used to examine the possibility of cyber security threats and vulnerabilities that the company can face. In Appendix B (section B.1), the author created a table where diverse sources of vulnerabilities and threats are reported. In the following subsections, vulnerabilities and threats are explained.

9.2.1 Vulnerabilities

Vulnerabilities have been defined as an imperfection in a system, device, service and its configuration, design or utilisation which enable a cybercriminal (in ABCD case) to perform a malicious activity such as access data without authorisation, use of cyber viruses or other kinds of cyber-attacks such as Distributed Denial of Service (DDoS)(Humayun, Niazi, Jhanjhi, Alshayeb, and Mahmood, 2020). In this report, the author identifies these sources of vulnerabilities:

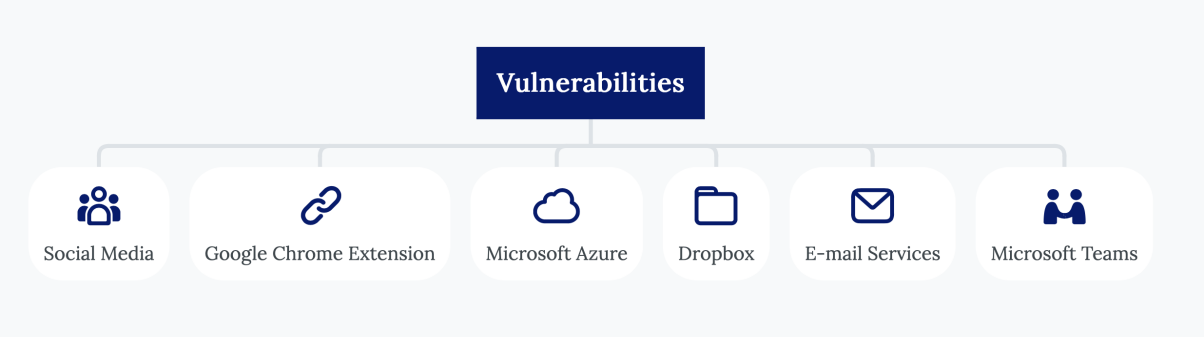

Figure 9.2: Vulnerabilities illustration Part 1

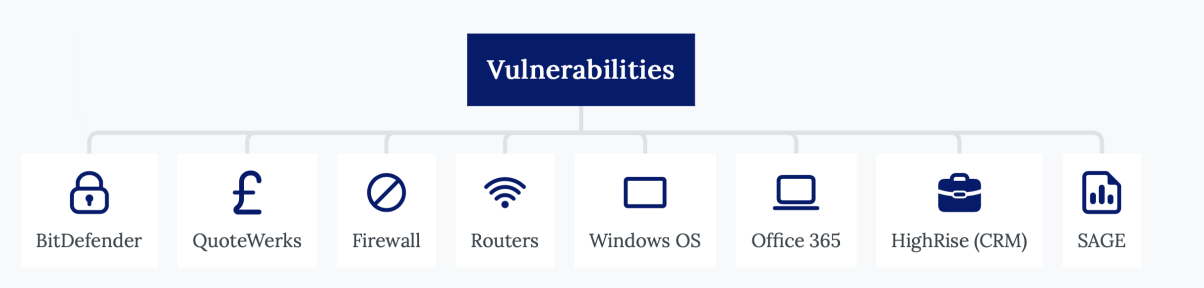

Figure 9.3: Vulnerabilities illustration Part 2

In Appendix B (section B.1), there has been described how it is possible to address the vulnerabilities' fundamental issues; it has been considered the possibility to put into practice these measures considering three parameters such as severity, occurrence, and detection. After evaluating these data, it is possible to create a list to prioritise the necessary anticipation measures that need to take place (See Appendix B, section B.1).

9.2.2 Threats

Threats are defined as actions that cyber criminals execute to achieve their intended goals or purposes (Humayun et al., 2020). These actions are possible since they are enacted using one or more exploited vulnerabilities. In Appendix B (section B.1), a table describing how to prevent

the exploitation of the vulnerabilities detected during the examination has been reported. To sum up, the threats determined by the author's analysis are:

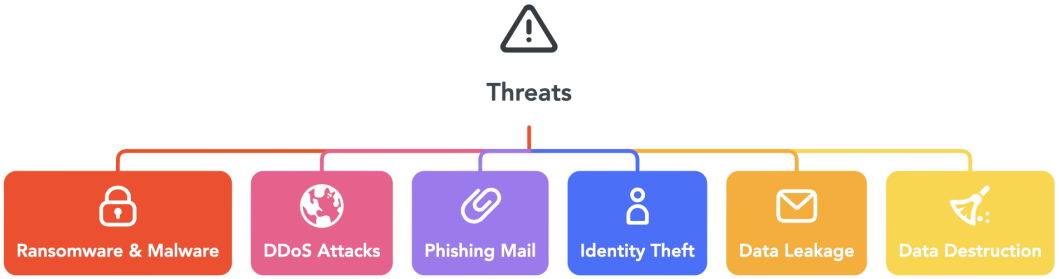

Figure 9.4: Threats illustration

These threats analysed in this document are related to cyber security and physical attacks. Cyber-attacks are the action of trying to impair, derange or infiltrate into computer systems, devices or networks using computerised tools (*NCSC glossary* 2016). Moreover, cyber-attacks are not built with the same characteristics, and their effects can vary; these unique features represent an enormous difficulty, considering that it is extremely hard to quantify with precision the destruction caused by these kinds of attacks (Rid and Buchanan, 2015).). On the other hand, cyber-physical attacks influence a physical unit of a system; this influence is not only related to intellectual property theft but could be, for example, the installation of malware via a USB port. In the manufacturing sector, these attacks are typically related to the alteration of designs or destruction of equipment (Elhabashy, Wells, and Camelio, 2019).

Chapter 10

Company Cyber and Information Security new Policy

After the investigation of the company via the adoption of two risk assessment standards, the author is going to explain the next steps necessary to improve security aspects.

10.1 Technical Aspects

In general, the company's choices of hardware and software are remarkable, considering their costs and benefits. The choices taken by the IT manager can confer a good reliable cyber security structure to the company. From the author's analysis, there are no situations that require an immediate change; nevertheless, it is advisable to change for cybersecurity reasons the HighRise software considering that it receives only security patches and is not under active development.

10.2 Human Factors

Humans are part of the company environment, the central core of its business activities, and their behaviour can influence this environment. Despite having clever work and cyber-culture, there is a necessity for the management to think about the chance of insider threat attacks. Insider threats represent a massive vulnerability in companies nowadays, considering that it is hard to detect and stop them. It is advisable to regulate the use of social media and personal devices in the workplace (Murire, Flowerday, Strydom, and J.S. Fourie, 2021), alongside the necessity to block the use of USB ports from employees; USB ports are a sensational channel for delivering cyber-attacks (See Chapter 7, section 7.2).

10.3 Physical Security measures

Where necessary, it is prudent to install RFID cards that can block unauthorised people from entering specific areas of the company (e.g., desktop station). Moreover, CCTV can be helpful in increasing the security of facilities (Costin, 2016). Before implementing these measures, a cost-benefit analysis should be done (Khoo and Cheng, 2011).

10.4 Identification and authentication technologies to improve information security

Looking at future improvements, it is necessary to discuss identification and authentication technologies which can improve the information security level. A solution can be implementing and utilising identity and access management (IAM).

10.4.1 The use of Blockchain Technology in Identity and Access Management (IAM)

The utilisation of blockchain technology can be a useful resource to prevent, mitigate and fight the risk of threats, especially insider threats. IAM represents a suitable option for ABCD to enhance its protection against this kind of attack (Nuss, Puchta, and Kunz, 2018). ABCD can use the concept and application of digital identity (DI) to enhance its security. DI can be composed of four categories as Identifier hash value, Identity signature, Storage pointer and Key pairs. Below, an example of digital identity is given.

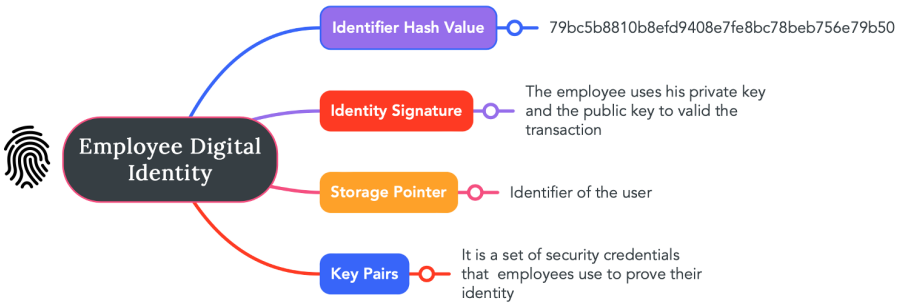

Figure 10.1: Graphic illustration of the employee digital identity

Once the DI has been created, it will be stored in a tamper-proof blockchain and is going to be used for validation. Whereas there is a necessity to update or revoke an owner's identity, it has been shown that can be easily performed (Nuss, Puchta, and Kunz, 2018).

Chapter 11

Briefly Business Continuity and Disaster Recovery plan

After performing a risk information security management assessment, a Business Continuity plan (BCP) and Disaster Recovery Plan (DRP) have been redacted; this action has been necessary to provide solutions to the company during business disruptions.

11.1 Business Continuity Plan (BCP)

BCP is the company's ability to manage and recover its business activities from unforeseen situations; these circumstances arise outside the sphere of DRP (Fani and Subiadi, 2019). This document will give instructions to respond to threats and disasters; it has been shown that organisations without a BCP succumbed to data breaches, wasting resources, and more severely closing their activities (Fani and Subiadi, 2019). BCP is designed to allow the organisation to continue operations while these unforeseen events are overseen.

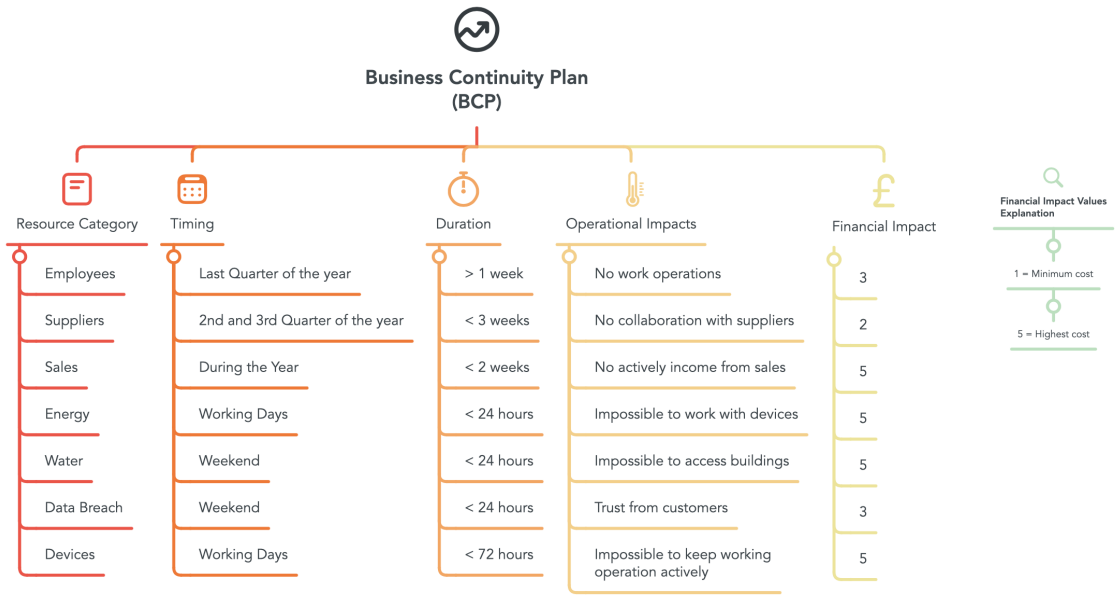

Figure 11.1: Business Continuity Plan

In figure 11.1, it is possible to see the BCP redacted by the author. The analysis conducted by the author shows that there have been identified seven categories which, if disrupted, can impact the company's business activities. Two key areas that need particular attention are:

- Duration of activities disservice (DoAS)
- The impact on the financial situation (FS)

DoAS is a vital parameter to study because knowing how long the company can operate without a specific area makes a difference in business survival. The FS dimension represents an area of concern considering the importance of cost for business; an estimation of cost could lead to better business solutions in the phase of recovery decision (Osadchy and Akhmetshin, 2015).

11.2 Disaster Recovery Plan (DRP)

DRP gathers, in a document, different recovery strategies to restore quickly and adequately IT operations after being disrupted (Fallara, 2004). Redacting this document involves taking decisions regarding:

1. Cost
2. Security
3. Time

Moreover, the DRP must embody ABCD operational requirements, and categories of systems and devices to regulate the conditions and priorities of the DRP (Fallara, 2004). Examples of these tools can include:

- Machinery replacement
- Backup Services and Methods
- Personnel training
- Testing systems periodically

In ABCD's DRP, the author has studied six different parameters, which include:

1. Critical system
2. Cost
3. Threat
4. Prevention Strategy
5. Response Strategy
6. Recovery Strategy

The cost category which is evaluated with a value between 1 and 5 (where 1 is the minimum cost and 5 is the maximum), its the one that gives a quantified idea about the impact of failure concerning the company.

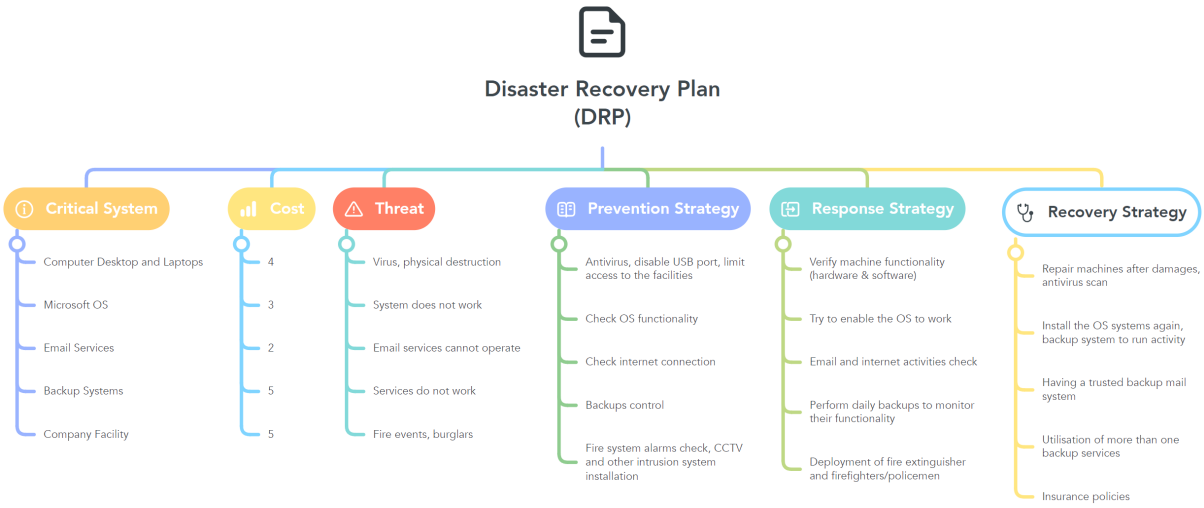

Figure 11.2: Disaster Recovery Plan

Chapter 12

Conclusion

The scope of this report is to analyse the Information Security structure of company ABCD. After utilising two risks assessment standards OCTAVE Allegro for a general purpose and FMEA for vulnerabilities and threats examination, it has been possible to state that:

1. ABCD has a good cyber structure
2. Mitigation and Anticipation tools (e.g., Azure, Dropbox, Microsoft OS, Firewall, two networks' areas) concerning cyber-attacks adopted by ABCD are well structured, and they perform well
3. Software used by the company can increase its security (e.g., Legal software, Assistance from Software houses)
4. There is a good cyber and computing culture within ABCD
5. Defined Roles within the company represent a huge advantage in critical situations
6. It is advisable to switch from HighRise software to another one for the reasons reported in Chapter 10 and Appendix B (section B.1)
7. Human factors (e.g., Insider threats) and Physical security represent perils for ABCD

In Chapter 10, a new policy is suggested by the author after his company's evaluation. Furthermore, the areas identified in Point 7, of the above list, constitute hazards for ABCD; consequently, suggestions to increase the security levels have been given in Chapter 10. Thus, an IAM solution has been proposed to increase identification and authentication in the company; this feature can be used for future improvement. Having good strategies in times of business disruption or even worse during disasters represents a crucial requirement for nowadays business; for these reasons, it has been counselled BCP and DRP in chapter 11. To sum up, ABCD is well equipped to address cyber security problems whereas suggestions to increase the level of security have been recommended in this document.

Bibliography

Albert, C. and Dorofee, A. J. (2001). 'OCTAVE criteria, Version 2.0'.

Amara, N., Landry, R., and Traoré, N. (2008). 'Managing the protection of innovations in knowledge-intensive business services'. *Research Policy*, 37.(9), pp. 1530–1547. ISSN: 0048-7333. doi: https://doi.org/10.1016/j.respol.2008.07.001. Available at: https://www.sciencedirect.com/science/article/pii/S0048733308001509.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2017). 'Gender difference and employees' cybersecurity behaviors'. *Computers in Human Behavior*, 69, pp. 437–443. ISSN: 0747-5632. doi: https://doi.org/10.1016/j.chb.2016.12.040. Available at: https://www.sciencedirect.com/science/article/pii/S0747563216308688.

ASQ (2005). *Failure Mode And Effects Analysis (FMEA)*. Available at: https://asq.org/quality-resources/fmea.

Blakley, B., McDermott, E., and Geer, D. (2001). 'Information Security is Information Risk Management'. *Proceedings of the 2001 Workshop on New Security Paradigms*. NSPW '01. Cloudcroft, New Mexico: Association for Computing Machinery, 97–104. ISBN: 1581134576. doi: 10.1145/508171.508187. Available at: https://doi.org/10.1145/508171.508187.

Caralli, R. A., Stevens, J. F., Young, L. R., and Wilson, W. R. (2007). *Introducing octave allegro: Improving the information security risk assessment process*. Tech. rep. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst.

Costin, A. (2016). 'Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations'. *Proceedings of the 6th international workshop on trustworthy embedded devices*, pp. 45–54.

Elhabashy, A. E., Wells, L. J., and Camelio, J. A. (2019). 'Cyber-Physical Security Research Efforts in Manufacturing – A Literature Review'. *Procedia Manufacturing*, 34, pp. 921–931. ISSN: 2351-9789. Available at: https://www.sciencedirect.com/science/article/pii/S2351978919308431.

Everett, C. (2011). 'Is ISO 27001 worth it?' *Computer Fraud Security*, 2011.(1), pp. 5–7. ISSN: 1361-3723. doi: https://doi.org/10.1016/s1361-3723(11)70005-7. Available at: https://www.sciencedirect.com/science/article/pii/S1361372311700057.

Fallara, P. (2004). 'Disaster recovery planning'. *IEEE Potentials*, 23.(5), pp. 42–44. ISSN: 1558-1772. doi: 10.1109/mp.2004.1301248.

Fani, S. V. and Subiadi, A. P. (Oct. 2019). 'Trend of Business Continuity Plan: A Systematic Literature Review'. EAI. doi: 10.4108/eai.13-2-2019.2286164.

González-Herrero, A. and Smith, S. (2008). 'Crisis Communications Management on the Web: How Internet-Based Technologies are Changing the Way Public Relations Professionals Han-

dle Business Crises'. *Journal of Contingencies and Crisis Management*, 16.(3), pp. 143–153. doi: https://doi.org/10.1111/j.1468-5973.2008.00543.x. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-5973.2008.00543.x. Available at: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1468-5973.2008.00543.x.

Gutandjala, I., Gui, A., Maryam, S., and Mariani, V. (2019). 'Information System Risk Assessment And Management (Study Case at XYZ University)'. *2019 International Conference on Information Management and Technology (ICIMTech)*. Vol. 1, pp. 602–607. doi: 10.1109/icimtech.2019.8843748.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., and Mahmood, S. (2020). 'Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study'. *Arabian Journal for Science and Engineering*, 45.(4), pp. 3171–3189. ISSN: 2191-4281. doi: 10.1007/s13369-019-04319-2. Available at: https://doi.org/10.1007/s13369-019-04319-2.

Khoo, B. and Cheng, Y. (2011). 'Using RFID for anti-theft in a Chinese electrical supply company: A cost-benefit analysis'. *2011 Wireless Telecommunications Symposium (WTS)*. IEEE, pp. 1–6.

Murire, O. T., Flowerday, S., Strydom, K., and J.S. Fourie, C. (2021). 'Narrative review : social media use by employees and the risk to institutional and personal information security compliance in South Africa'. *TD : The Journal for Transdisciplinary Research in Southern Africa*, 17.(1), pp. 1–10. doi: 10.4102/td.v17i1.909. eprint: https://journals.co.za/doi/pdf/10.4102/td.v17i1.909. Available at: https://journals.co.za/doi/abs/10.4102/td.v17i1.909.

NCSC glossary (Nov. 2016). en. https://www.ncsc.gov.uk/information/ncsc-glossary. Accessed: 2023-1-16.

Nissim, N., Yahalom, R., and Elovici, Y. (2017). 'USB-based attacks'. *Computers Security*, 70, pp. 675–688. ISSN: 0167-4048. doi: https://doi.org/10.1016/j.cose.2017.08.002. Available at: https://www.sciencedirect.com/science/article/pii/S0167404817301578.

Nuss, M., Puchta, A., and Kunz, M. (2018). 'Towards Blockchain-Based Identity and Access Management for Internet of Things in Enterprises'. *Trust, Privacy and Security in Digital Business*. Ed. by S. Furnell, H. Mouratidis, and G. Pernul. Cham: Springer International Publishing, pp. 167–181. ISBN: 978-3-319-98385-1. Available at: https://link.springer.com/chapter/10.1007/978-3-319-98385-1_12.

Nyanchama, M. (2005). 'Enterprise Vulnerability Management and Its Role in Information Security Management'. *Information Systems Security*, 14.(3), pp. 29–56. doi: 10.1201/1086.1065898x/45390.14.3.20050701/89149.6. eprint: https://doi.org/10.1201/1086.1065898X/45390.14.3.20050701/89149.6. Available at: https://doi.org/10.1201/1086.1065898X/45390.14.3.20050701/89149.6.

Osadchy, E. A. and Akhmetshin, E. M. (2015). 'Development of the financial control system in the company in crisis'. *Mediterranean Journal of Social Sciences*, 6.(5), p. 390.

Pousttchi, K., Gleiss, A., Buzzi, B., and Kohlhagen, M. (2019). 'Technology Impact Types for Digital Transformation'. *2019 IEEE 21st Conference on Business Informatics (CBI)*. Vol. 01, pp. 487–494. doi: 10.1109/cbi.2019.00063.

Rid, T. and Buchanan, B. (2015). 'Attributing Cyber Attacks'. *Journal of Strategic Studies*, 38.(1-2), pp. 4–37. ISSN: 0140-2390. doi: 10.1080/01402390.2014.977382. Available at: https://doi.org/10.1080/01402390.2014.977382.

Sardjono, W. and Cholik, M. I. (2018). 'Information Systems Risk Analysis Using Octave Allegro Method Based at Deutsche Bank'. *2018 International Conference on Information Management and Technology (ICIMTech)*, pp. 38–42. doi: 10.1109/icimtech.2018.8528108.

Schmittner, C., Gruber, T., Puschner, P., and Schoitsch, E. (2014). 'Security application of failure mode and effect analysis (FMEA)'. *International conference on computer safety, reliability, and security*. Springer, pp. 310–325.

Tankard, C. (2016). 'What the GDPR means for businesses'. *Network Security*, 2016.(6), pp. 5–8. ISSN: 1353-4858. doi: https://doi.org/10.1016/s1353-4858(16)30056-3. Available at: https://www.sciencedirect.com/science/article/pii/S1353485816300563.

Weis, S. A. (2007). 'RFID (radio frequency identification): Principles and applications'. *System*, 2.(3), pp. 1–23.

Zheng, Y., Li, Z., Xu, X., and Zhao, Q. (2022). 'Dynamic defenses in cyber security: Techniques, methods and challenges'. *Digital Communications and Networks*, 8.(4), pp. 422–435. ISSN: 2352-8648. doi: https://doi.org/10.1016/j.dcan.2021.07.006. Available at: https://www.sciencedirect.com/science/article/pii/S235286482100047X.

Appendices

Appendix A

OCTAVE Allegro

A.1 Establish risk measurement criteria, part 1

Impact Area	Low	Medium	High
Customer Trust	Reduction of customer trust after communicating a cyber breach and explaining the following security measures are less than 10%	Reduction of customer trust after communicating a cyber breach but not explaining the following procedures to contain the risk is between 40% and 60%	Reduction of customers trust due to lack of communication after a cyber-attack more than 80%
Employees	Training employees and helping them to understand the risk of cyber-attacks enhance the probability of reducing successful cyber attacks	Training employees could improve the probability of reducing successful cyber attacks	No training employees and helping them to understand the risk of cyber-attacks enhance the probability of successful cyber-attacks against the company
Policies	A well-written cyber security policy which contains procedures, technological safety, and operational countermeasures in case of cybersecurity incidents reduce the risks of successful cyber attacks	A cyber security policy which contains only procedures and operational countermeasures in case of cybersecurity incidents might be able to reduce some risks related to cyber-attacks	A cyber security policy which contains only procedures in case of cybersecurity incidents cannot be able to reduce the risks of successful cyber attacks
Suppliers	In case of an established agreement concerning the utilisation of data, sharing of data, the risks of losing information are minimised lower than 10%	In case of an established agreement concerning only the utilisation of data, the risks of losing information are decreased between 20% and 30%	In case of an established agreement concerning the utilisation of data, the share of data does not exist, the risks of losing information are increased more than 50%

Table A.1: Establish Drivers Phase - Establish Risk Measurement Criteria, First Part

A.2 Establish risk measurement criteria, part 2

Impact Area	Low	Medium	High
Devices	Protecting, company devices with hardware and software solutions, can minimise the chance of successful cyber attacks	Protecting company devices with only software solutions can decrease the chance of successful cyber attacks	No protecting company devices with hardware and software solutions can increase the chance of a successful cyber attack above 90%
Network	Connecting devices via a mixture of wired-wireless connections, utilising firewall and WPA2 protection, having different networks for company members and guests can minimise below 5% the risk of successful cyber attacks	Connecting devices via a mixture of wired-wireless connections, utilising firewall and WPA2 protection can minimise below 35% the risk of successful cyber attacks	No connecting devices via a mixture of wired-wireless connections, utilising firewall and WPA2 protection, having different networks for company members and guest can increase above 90% the risk of a successful cyber attack
Software	Purchasing legal software and license, updating, and patching regularly software can decrease below 10% the probability of a successful cyber attack	Updating and regularly patching software can decrease below 40% the probability of a successful cyber attack	No purchasing legal software and licenses, updating and patching regularly software can increase above 85% the probability of a successful cyber attack

Table A.2: Establish Drivers Phase - Establish Risk Measurement Criteria, Second Part

A.3 Critical assets table

Critical Asset	Rationale for Selection	Description of Consequence
Customer Trust	Leakage of information regarding customers can impact their trust in the company; this can lead to legal issues	Data and information of customers such as name, address, telephone numbers and billing details
Employees	Leakage of employee information can impact the functionality of the company because cyber threats can emerge	They are the centre of the company; information regarding them must be protected from external and internal threats
Policies	Knowing the policies of the company can represent an advantage for criminals considering their ability to enhance their attacks	Policies regulate procedures, technological safety, and operational countermeasures in case of cybersecurity incidents
Suppliers	Leakage of agreements and contracts between the company and suppliers can damage their business activities, and operability	Agreement and contracts with suppliers are vital for the company to be operable
Devices and Software	LLeakage of information regarding devices and software used by the company can enrich the knowledge of cybercriminals to conduct their bespoke attacks	The company uses devices and software to conduct their activities and to store data
Network	Compromising the operability of the network or destabilise its operability can impact how information is transported and used	Network has a huge role in helping the company to conduct its business

Table A.3: Profiling and identifying Assets

Appendix B

FMEA

B.1 FMEA model representation

Process Step/Input	Potential Failure Mode	Potential Failure Effects	SEVERITY (1 - 10)	Potential Causes	OCCURRENCE (1 - 10)	Current Controls	DETECTION (1 - 10)	RPN	Action Recommended	Resp.
What is the process step, change or feature under investigation?	In what ways could the step, change or feature go wrong?	What is the impact on the customer if this failure is not prevented or corrected?		What causes the step, change or feature to go wrong? (how could it occur?)		What controls exist that either prevent or detect the failure?			What are the recommended actions for reducing the occurrence of the cause or improving detection?	Who is responsible for making sure the actions are completed?
Use of social media	Gathering information	None	6	Employees do not pay attention online	8	Regulating social media uses by employees	8	384	Blocking social media uses from work devices and network	IT manager
Google Chrome Extensions	Installation of malicious extension	Propagation of cyber virus	8	Employees do not pay attention on the extensions	10	Downloading only certain kind of extensions	7	560	Allowing only extensions that have been checked by the IT manager	IT manager
Backup Data with Azure	Backup does not work	Losing working data	9	Failure of the backup system/ no network connection	10	Checking the functionality of this service	5	450	Backup data regularly during the day to minimise the chance of a failure	IT manager
Backup Data with Dropbox	Backup does not work	Losing working data	9	Failure of the backup system/ no network connection	10	Checking the functionality of this service	5	450	Backup data regularly during the day to minimise the chance of a failure	IT manager
E-mail services	Leaked email, identity theft	Identity theft, leakage of confidential conversation and data	9	Receiving a phishing mail	6	Mail filters, warning about the email is originated outside the organisation	3	162	Training employees to recognise phishing email	Employees
Use of Microsoft Teams	Identity theft, uploading of malicious contents	Identity theft, propagation of cyber virus	5	Stealing access credential of the service	1	Protecting accounts access with 2AF	7	35	Training employees to recognise phishing email or other techniques used by criminals to steal credentials	Employees
Use of QuoteWerks software	System does not work	Could not receive price estimation	6	Failing on integrating the system	5	Read documentation to allow the system to work	1	30	Studying the documentation to enhance a correct system configuration	IT manager
Firewall	Not configuring the firewall in a optimal way	None	8	Configuring the firewall not in the right way	1	Testing the firewall configuration and resilience	3	24	Studying and improving the configuration of the firewall	IT manager
Routers	Not configuring the security of the routers	None	7	Configuring the routers not in the right way	1	Testing the router configuration	3	21	Studying and improving the configuration of the routers	IT manager
Windows 10 Professional	Attack successful using an OS vulnerability	None	10	Not updating the OS regurarly	3	Updating Microsoft Windows OS regularly	6	180	Using Microsoft Windows update services regularly and reminders	IT manager
Office 365	Attack successful using a vulnerability using one the macros of Office 365	Cyber attacks using files originated from this service	10	Not updating the sofware regurarly / enabling macros	3	Updating Office 365 regularly	7	210	Using Office 365 update services regularly and reminders	IT manager
HighRise (CRM System)	Not being under active development	Leakage of clients data	6	The service does not receive security patches	2	Updating security with patches	6	72	Trying to update the service regurarly or change CRM system	IT manager
SAGE (Financial information service)	Software house does not address security problem	Leakage of customers data	7	The service does not receive security updates	2	Updating security with patches	4	56	Trying to update the service regurarly	IT manager
Bitdefender	Not updating the system, no configuring the system in the most appropriate way	None	10	The system cannot perform antivirus analysis	1	Updating the system in regular base	8	80	Trying to update the service regurarly	IT manager

Figure B.1: FMEA illustration