University College London

Department of Information Studies

Business report

Module leader:

Dr Elizabeth Lomas

This Business Report is submitted as an assessment for INST0057: Information Governance

Student ID: 19075478

Word count: 2159

May 3rd 2020

Table of contents

1. Executive Summary

As a trusted advisor, I deliver Business report accompanied by Risk register to enable you to make informed decisions about Information Security that support your business objectives. Your company rely on IT systems to support all of your crucial business processes. To adequately address this issue, in the supplied Risk register I have examined, that this dependence may lead to (1) digital threats such as cyber attacks or hacking and (2) physical threats such as information loss, physical damage and deterioration. Therefore, I created the Risk register to protect all your IT systems and procedures that contain essential data. In this report, I also included an overview of vulnerabilities and other exposures that can leave organisations and users exposed to infringement or attack. I analysed several approaches to mitigate such threats and supplied Risk management implementation plan, which would take into account the use of PDCA method. Stakeholders must identify the changes in threat techniques so that they can adapt their security practises and protect your users. Points raised in this report include significant advances in malicious code, changes in web attack methods, spyware, Business Email Compromise (BEC). Poor security practises, such as not taking a step to mitigate identified vulnerabilities, not controlling access to cloud services, and maintaining networks and endpoints unmanaged, are mentioned along with their financial and operational consequences.

2. Organization

2.1. Introduction

Webdos is a newly founded company established in January 2019. Within 12 months, Webdos became one of the largest provider of web hosting services in the UK. Webdos has its private data centre, where only servers are located and is building a second data centre. Webdos is not afraid to invest in technology, innovation and research so that they can provide services to the broadest possible public. It is necessary to comply with the latest risk management standards. Webdos aims to deliver quick, secure domain registrations and web hosting services that make it easier to build an online presence. Technicians at Webdos have a wide variety of skills and are competent on several specific technological issues, which means looking beyond what hosting companies usually provide. Webdos agree that policies and regulations must adhere especially in the web-based world.

3. Supplied Risk register Overview

3. 1. Approach and structure

This Business report aims to advise your company of significant information risks which can be found in the offered Risk register. Significant threats are those that pose a challenge to the systems, business models or sustainability of Webdos and its operating data centres (V. Benjamin, et al., 2015). This Risk register represents those risks that matter the most, thus should have a risk treatment plan in place. As part of the Risk register, critical operational risks, strategic risk and market performance threats are outlined. The findings of this Risk register shall be followed up.

The offered Risk register lays out:

- The general risk policies and limits for all forms of information risk
- The general risk management and control guidelines
- Periodically reviews the risk policies and limitations

You shall mitigate significant risks that could expose long-term objectives, which demonstrated in the supplied Risk register, such as:

- Unauthorized access to the information system (internal & external)
- Malicious code attack
- Software/hardware errors, natural disasters, power outages
- Damage caused by a third party
- Breach of contractual relations
- Information loss, physical damage or deterioration
- Poor information management
- Disclosure of information
- Network user attack (internal employee)
- Failure to exploit business information
- Inaccurate information

Individual risks and their impact are represented in the following Risk level categories:

- Impact
- Likelihood
- Risk score
- Evaluation

3. 2. ISO 27001

Risk is about the "impact of uncertainty on goals," and if you know how to handle uncertainty, you can effectively reduce the risk in your company. In terms of the ISO 27001 standard, this ensures that information can be easily secured and used to help an organisation achieve its objectives. Through consistently defining, reviewing, assessing and handling a detailed list of related risks, undesired circumstances can be avoided, and negative impacts reduced (ISO, 2020) (Giesler, 2019). As you can see in Figure 1, by identifying and applying risk reduction, you can effectively find out about possible problems before they happen. In other words, ISO 27001 risk reduction is a reminder: better safe than sorry.

Information assets for the purpose of ISO 27001 risk assessment include:

- Data, information, records
- Software
- Hardware
- Services/Utilities
- People, their qualification skills
- Intangibles (reputation and image)

Figure 1. ISO 27001 Information Security (Rheinland, 2020)

3. 3. Confidentiality, integrity and availability (CIA)

Confidentiality, integrity and availability (CIA Framework) are the three dimensions of information security (G. Yan & Weigle, 2009). It is essential to ensure that you deal with them correctly thus I align them in the Risk register to protect your information capital. Figure 2 presents the three main elements that are supporting the Risk register in an effective information security policy.

Additionally, you may not consider your information sensitive or a possible target of an attack yet. However in today's Internet world without borders, disrupting IT processes can suspend your operations and allow your competition to earn an advantage in the market in a matter of seconds (Noroozian, et al., 2015), (G. Yan & Weigle, 2009).

To conclude the above, supplied Risk register offers a systematic and well-structured approach that will protect:

- the **confidentiality** of your information
- ensure the **integrity** of business data
- improve the **availability** of your IT systems.

Figure 2. The CIA triad (Purcell, 2018)

4. Risk Management Implementation

4. 1. Plan-Do-Check-Act (PDCA) Cycle

This cyclical strategy is the foundation of risk management framework ISO 27001 (2005), which promotes a quality improvement approach by a cycle of developing, enforcing, tracking, evaluating and enhancing the information security management structure (Nicho, 2018). Hence, I advise the implementation of the risk management framework through the prism of Edward Deming's PDCA method. Successful application of information security requires the use of a structural combination of: IT control structures (which match IT priorities with corporate objectives), IT process management (which ensures stable and productive business continuity), and compliance with applicable safety requirements, regulations and programmes (Nicho, 2018), (Choobineh, et al., 2007). All components assure that the confidentiality, credibility and availability (CIA) of your assets are protected at all times.

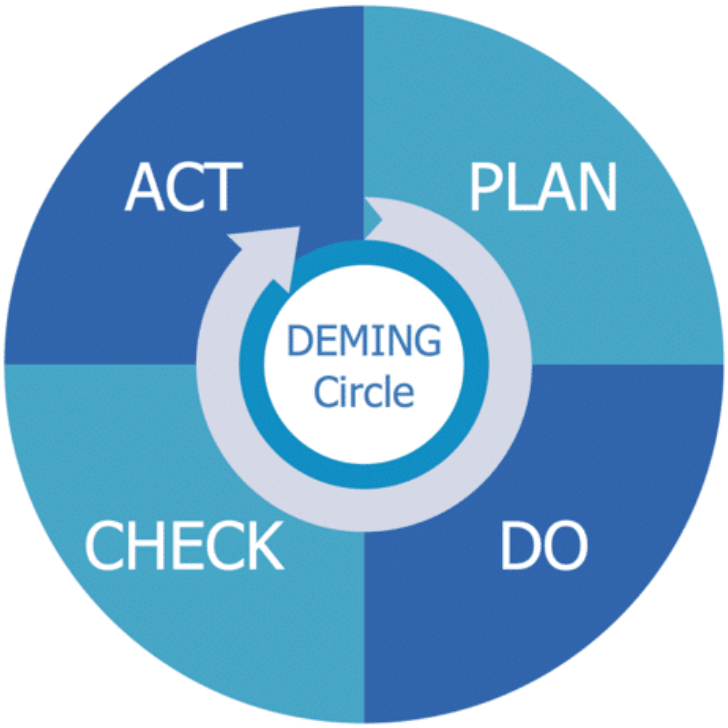

Figure 3. The PDCA Circle (Thomson, 2019)

PDCA method of ISO 27001 implementation consist of 4 phases:

- **Plan:** The planning stage of implementing ISO 27001 begins with risk assessment, followed by the phases: policy definition, requirements delineation, control establishment (Choobineh et al., 2010).

- **Do:** Managers will implement a protection system that involves the use of a risk controls model, security education and counter measurement matrix analysis. Mapping of suitable

IT controls concerning ISO 2700 structures and standards (Choobineh, et al., 2007).

- **Check:** Inspections of implemented Risk maangement play a crucial role in risk mitigation, as 97 percent of breaches may be prevented by regular security controls (Nicho, 2018).This phase consists of the measurement and monitoring of security management structure by using key performance indicators.

- **Act:** Implementation ISO 27001 process involves the integration and mapping of relevant IT structures and standards. Stakeholders involved in the implementation phase share a culture of protection through continuous security training by applying the best practices of the industry to incorporate ISO 27001 at every point of the PDCA process. (Nicho, 2018).

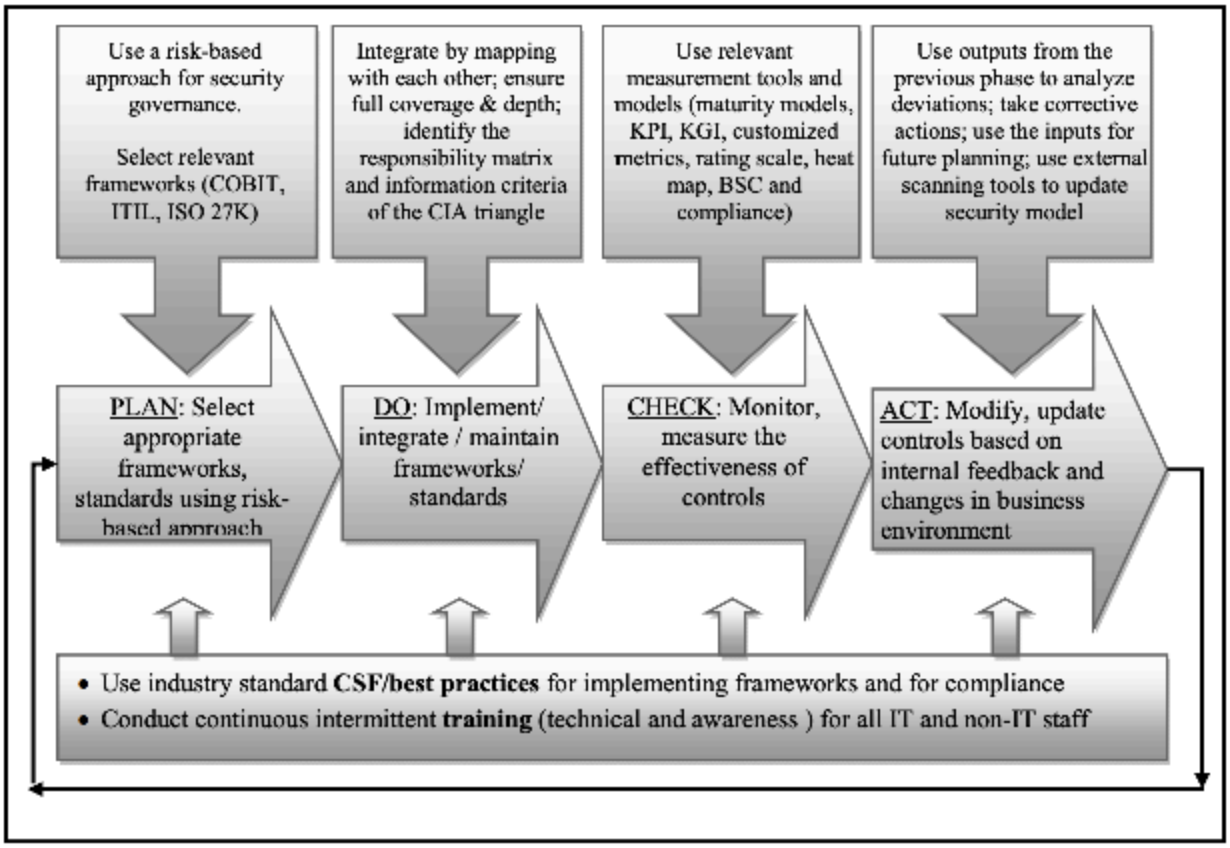

Figure 4. Risk management Implementation process model (Nicho, 2018).

5. Risk Management Goals and Objectives

Your customer data, as well as your know-how, which is the core of the business, need protection. For you, as a newly founded company is the risk of potential damage particularly crucial as it may affect your reputation that could occur as a result of inadequate risk management or security breaches (Noroozian, et al., 2015). These incidents could ruin the chances of your success and would seriously expose the path of your business development. Data handling – particularly in your IT-driven company – shall be the norm, not the exception. Increasingly sophisticated attacs can come from organisations, individuals or foreign intelligence services (Ullrich, et al., 2012), (Negrete-Pincetic, et al., 2009) (Ablon, et al., 2016). You can suffer severe injuries, including financial consequences and damage to reputation, as 1 minute of server downtime can cost you up to £7000 (Topi & Tucker, 2014), (Galligan, 2016). Hence, I suggest you to take into account the three following aspects of to ensure the success and reputation of your company in the future.

5.1 Processes and strategies

In risk management, processes and strategies are critical to the effective business activities and operational processes. In the supplied Risk register, I am suggesting you a consistent context for understanding IT threats, compliance procedures and core operating features, such as:

- How IT applications will be held up to date
- Anti-virus implication
- Data collection and backups
- IT change management
- Employee training
- Review access rights and permission settings
- File tracking procedures

All of the mentioned specifications play a significant role in your business process and strategies and are related to the production, monitoring, operating environments, vulnerability protection and knowledge recovery.

The primary business activities need to comply with the suggested Risk register, that will result in more explicit reporting. It ensures that all your workers can have specific instructions to follow, which will help to maintain the organisation secure and minimise the risk. These could involve rules relating to the usage of servers, firewall implication, digital signatures, timestamps or strong passwords (Farhat, et al., 2017), (Choobineh, et al., 2007). I encourage you a systematic approach to risk management as it includes the development and distribution of resources in the right place, in the right way and at the right time. It was taking into account not only the needs of your company, but also those of its customers and other stakeholders. As demonstrated, the overall risk score of controlled external cyber-attacks is thanks to the risk register lowered to its minimum and business processes enhanced to work more efficiently.

5.2 Compliance and Fines prevention

Compliance in business brings not only prevention form criminal charges, building a positive reputation but also higher productivity in the company. Obeying the regulations of a company's market is essential to the survival and growth of your company. It is crucial for you, as a young and more vulnerable company, to avoid fines and obstacles that would make a further grow even more challenging (Arbel, 2015). I am recommend you to show enforcement in the case of an accident. Thus compliance has to be protected. The aim is to prevent infringements of regulatory or contractual obligations concerning safety and security of information.

The supplied Risk register successfully explains how to clearly define, record and amend the applicable legislative, administrative, contractual specifications and the strategy of your company to fulfil certain criteria within each information system and entity. As proved in the risk register, the likelihood of controlled both internal and external attacks is lowered, and the financial and legal consequences are minimized.

5.3 Competitive advantage & reputation

TThe prestige of Webdos is a critical component of the success of their mission. Customers want their data safe and stable. Although the return on investment from the information security management framework may be high, the initial investment triggers usually come from outside factors such as essential customers. The alignment of your company with the expectations and requirements of your customers will give you a strategic advantage and make you a much more appealing prospect (Telang & S. Wattal, 2007).

Regarding your reputation, the supplied Risk register might have an impact on:

- An increase in the company's image
- Visibility within the competition
- Enables faster adaptation of your company to the changing requirements of customers
- Strengthening how the company is viewed by the customers, vendors and other stakeholders
- Improves the organization's infrastructure, governance and day-to-day processes.

6. Risk Appetite

Risk appetite refers to how much risk you are able to face to achieve the business objectives. (Hillson & Murray-Webster, 2012). The risk appetite system provides an overview of different risk dimensions and helps you to control risk assessment across certain dimensions in compliance with its overall risk policies (Cremonino, 2011). Figure 3 shows suggested comprehensive structure that is used to express risk appetite. I advise defining, evaluating and managing risks within the context of risk management, ensuring that risks are identified and handled efficiently in order to achieve your objectives. Although you are seeking creativity and change, Webdos shall not sacrifice its reputation in any manner.

Understandning your risk appetite:

- With a high risk appetite, even a risk measured as high can seem appealing if the potential profit is high enough
- Increased risk tolerance can expose you to more risks by making you use less strict controls in search of a particular opportunity, so test if the anticipated benefits from taking risks will pay or intermediate losses and still provide incentives reasoned desirable (Giesler, 2019).

Risk Type	Seeking	Tolerant	Neutral	Moderate	Averse
Research and development			☑		
Quality					☑
Security					☑
Data access				☑	
Innovation		☑			
Financial					☑
Business Change				☑	
Skills and Capability			☑		

Figure 5. Suggested Risk Appetite

7. Investment Required

Top management, technical personnel, final users, experts – all those involved in information security must have specified responsibilities (e.g. decision taking, risk assessment, follow-up procedures, etc.). This is one of the most cost-effective ways to minimise information security risks, as each person would know what is required of them (Kropp, 2006). For this reason, essential employee training is required and included in the investment forecast (figure 6). Figure 7 also demonstrates that modern technology reduces server cooling costs, new systems are user-friendly and contain fewer glitches and defects. Thus, it increases the workers' performance and lowers costs. When appropriately applied, it can optimise the production, reduce the capital needed, rapidly develop internal experience and build sustainable competitive advantage (Arthur, 1997), (Kropp, 2006). I also included financial and operational loss if risks remain uncontrolled (see figure 7).

Asset	Investment	Timescale
Employee training	>£30k	Annually
Malicious code alerting system	>£2000	Annually
Servers cooling solution upgrade	>£200k	Every 3 years upgrade
Security and protection solutions	>£10k	Annually
Hardware upgrade and maintenance	> £50k	Every 4 years upgrade

Figure 6. Investment forecast 2020

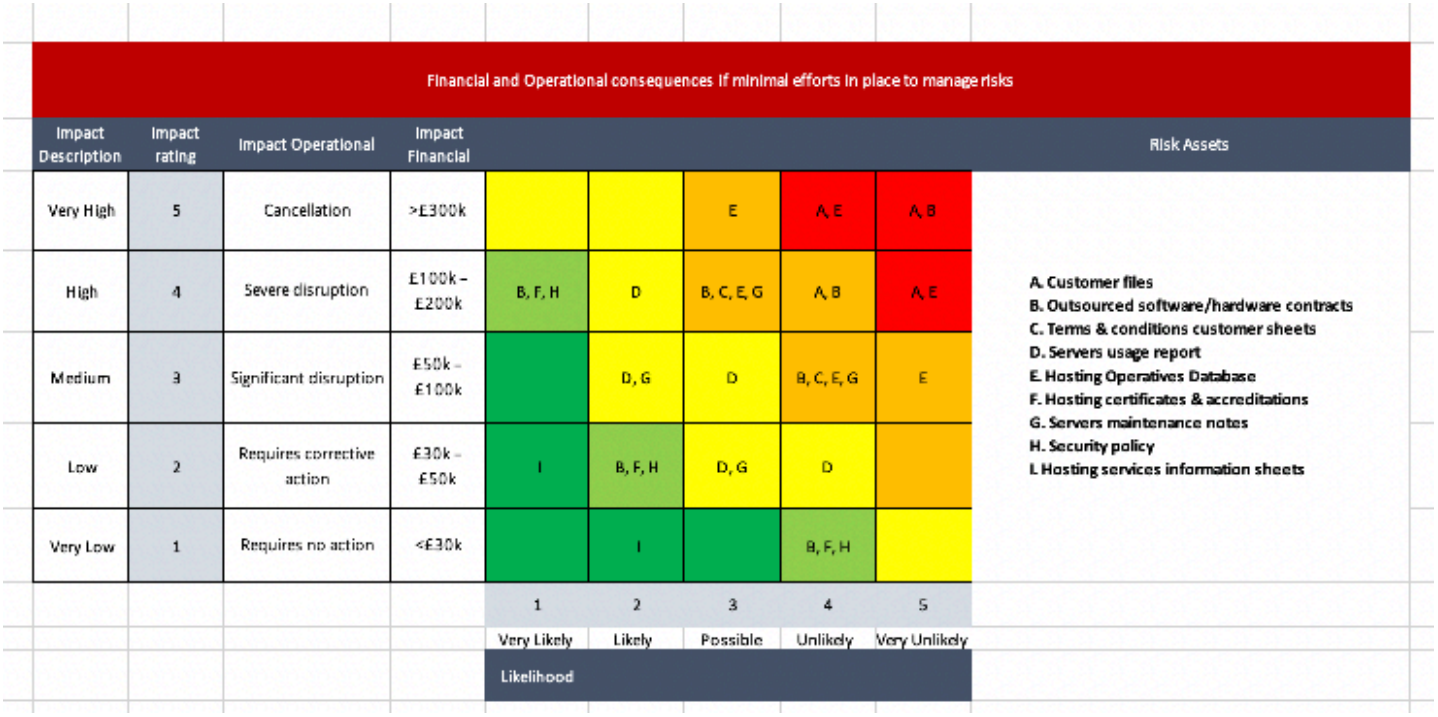

Figure 7. Forecasts of Financial and Operational loss if minimal efforts in place to manage risks

8. Final recommendations

Both security best practises, and risk management techniques have been thoroughly examined to have a good understanding of the primary challenges in the context of risk assessment. This risk assessment starts with the examination of risk assets, used to develop attack scenarios and detect potential vulnerabilities and threats. The Risk Register and its implementation is structured to address multiple security criteria and to provide you, as a decision-maker, with an ideal situation. Resulting in encouraging your IT Directors in defining the frameworks they should use to increase the efficiency of the information security management process. Your organization would also be able to show robust internal control on financial system. This method will complement the Plan, Do, Check, Act (PDCA) cycle, which is a commonly accepted framework for ISO 27001 certification. As observed in the supplied Risk register, your organization with ISO 27001 certification and verification would strengthen risk-based approach to information security management through an ongoing risk evaluation and risk mitigation phase. For this reason, I have sampled various risk assets and their mitigations procedures, which would result in increased company's profitability, reputation, savings, credibility and more effective operations. It is clear to us that opportunities for work in the field of information system security will continue to grow as our reliance on information technology increases.

9. Bibliography

Ablon, L. H. P., Lavery, D. C. & Romanosky, S., 2016. Consumer Attitudes Toward Data Breach Notifications and Loss of Personal Information. Santa Monica, Calif: RAND.

Arbel, L., 2015. Data loss prevention: the business case. Computer Fraud & Security, 2015(5), pp. 13-16.

Arthur, L. J., 1997. Quantum improvements in software system quality. Communications of the ACM, 40(6), pp. 46-52.

Choobineh, J., Dhillon, G., Grimaila, M. R. & Rees, J., 2007. Management of Information Security: Challenges and Research Directions. Communications of the Association for Information Systems, Volume 20.

Cremonino, A., 2011. Risk appetite as a core element of ERM: Definition and process. Enterprise Risk Management Symposium, Society of Actuaries, Chicago, pp. 1-29.

Farhat, V., McCarthy, B., Raysman, R. & Knight, L., 2017. Holland and Knight. [Online]
Available at: https://www.hklaw.com/files/Uploads/Documents/Articles/2017CyberAttacksPreventionandProactiveResponses.pdf
[Accessed 1 5 2020].

G. Yan, S. O. & Weigle, M. C., 2009. Providing location security in vehicular Ad Hoc networks. IEEE Wireless Communications, 16(6), pp. 48-55.

Galligan, D., 2016. Business Insider. [Online]
Available at: https://www.businessinsider.com/
[Accessed 29 4 2020].

Giesler, A., 2019. Advisera. [Online]
Available at: https://advisera.com/
[Accessed 28 4 2020].

Hillson, D. & Murray-Webster, R., 2012. A short guide to risk appetite. Farnham: Gower Publishing, Ltd.
ISO, 2020. ISO. [Online]
Available at: https://www.iso.org/
[Accessed 29 4 2020].

Kropp, T., 2006. System threats and vulnerabilities. IEEE Power and Energy Magazine, 4(2), pp. 46-50.

Negrete-Pincetic, M., Yoshida, F. & G. Gross, 2009. Towards quantifying the impacts of cyber attacks in the competitive electricity market environment. 2009 IEEE Bucharest PowerTech.

Nicho, M., 2018. A process model for implementing information systems security governance. Information and Computer Security, 26(1), pp. 10-38.

Noroozian, A. K. M., Tajalizadehkhoob, S. & Van Eeten, M., 2015. Developing security reputation metrics for hosting providers. Delft University of Technology.

Purcell, A., 2018. IBM. [Online]
Available at: https://www.ibm.com/blogs/cloud-computing/2018/01/16/drive-compliance-cloud/
[Accessed 28 5 2020].

Rheinland, T., 2020. TUV Rheinland. [Online]
Available at: https://www.tuv.com/turkey/en/iso-27001-certification.html
[Accessed 20 4 2020].

Telang, R. & S. Wattal, 2007. An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price. IEEE Transactions on Software Engineering, 33(8), pp. 544-557.

Thomson, J., 2019. Business Enterprise Mapping. [Online]
Available at: https://www.businessmapping.com/blog/the-effectiveness-of-the-plan-do-check-act-cycle/
[Accessed 29 4 2020].

Topi, H. & Tucker, A., 2014. Computing handbook: Information systems and information technology. third ed. s.l.:CRC press.

Ullrich, J. B., Kim, S. H. & Wang, Q.-H., 2012. A comparative study of cyberattacks. Communications of the ACM, 55(3), pp. 66-73.

V. Benjamin, W. L., Holt, T. & Chen, H., 2015. Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. IEEE International Conference on Intelligence and Security Informatics (ISI), Volume Baltimore, pp. pp. 85-90.