Cyber Security Risk Management

CSCI-530: Security Systems
Research Paper
Fall 2022

Name: Rishit Saiya
USC-ID: 4940905271
Email: rsaiya@usc.edu

I have read the Guide to Avoiding Plagiarism published by the student affairs office. I understand what is expected of me with respect to properly citing sources, and how to avoid representing the work of others as my own. The material in this paper was written by me, except for such material that is quoted or indented and properly cited to indicated the sources of the material. I understand that using the words of others, and simply tagging the sentence, paragraph, or section with a tag to the copied source does not constitute proper citation and that if such materiel is used verbatim or paraphrased it must be specifically conveyed (such as through the use of quotation marks or indentation) together with the citation. I further understand that overuse of properly cited quotations to avoid conveying the information in my own words, while it will not subject me to disciplinary action, does convey to the instructor that I do not understand the material enough to explain it in my own words, and will likely result in a lesser grade on the paper.

Signed: Rishit Saiya

Cyber Security Risk Management

Rishit Saiya
MS Cybersecurity
University of Southern California
rsaiya@usc.edu

***Abstract*—The threat of information security incidents is climbing. Risk Management authorities must consider their mitigation strategy in relation to the state-of-the-art threat landscape, existing security frameworks and global regulations to strategically manage these risks. With the rapidly increasing threats of information security, the following paper cover the prevalence, complexity and severity of high-risk attacks. According to latest reports, headlines have demonstrated a very high varied spectrum of attack methods. as well as the accompanying reputational damage. Today's growing network of connectivity only increases information risk, leaving organizations exposed and unprepared. This culminates in a massive Reputational, Technological damage and leading debt. This culminates in the conglomerates going through an ever-lasting impact of breach, legal liabilities, audit, probation, financial fines and deficit. This paper aims to provide a basic introduction the Cyber Risk, its implications, frameworks, regulations, compliance and some analysis on recent events.**

***Keywords* - Cyber Risk, NIST, Cybersecurity Frameworks, Risk Assessments, Governance, ISO, Incident Response**

I. Introduction

Incidents involving information security are becoming more frequent, sophisticated, and serious. Recent news stories highlight the range of targets and assault strategies, as well as the collateral reputational harm. Information risk only grows today as a result of the expanding network of connection, leaving firms vulnerable and unprepared. Few firms feel prepared to deal with information security crises in spite of this urgency. ERM (Enterprise Resource Planning) is in charge of managing and reducing risk as the second line of defense against information risk. Leaders in Risk Management must evaluate the threat environment and the most current legislative changes before deciding which information security framework best suits the goals and operations of their company. ERM may aid in reducing information risk by encouraging secure employee behavior, collaborating with the information security team, and building governance inside its business.

Some of the major findings have been:

- The foremost threat to a company's development, according to organizations, is information security, yet only 36% of boards claim to be adequately competent to assess and manage the organization's information risks.
- Information risk is amplified by four factors: insecure staff practices, sophisticated attacks, third-party vulnerabilities, and an expanding attack surface brought on by Internet of Things connections.

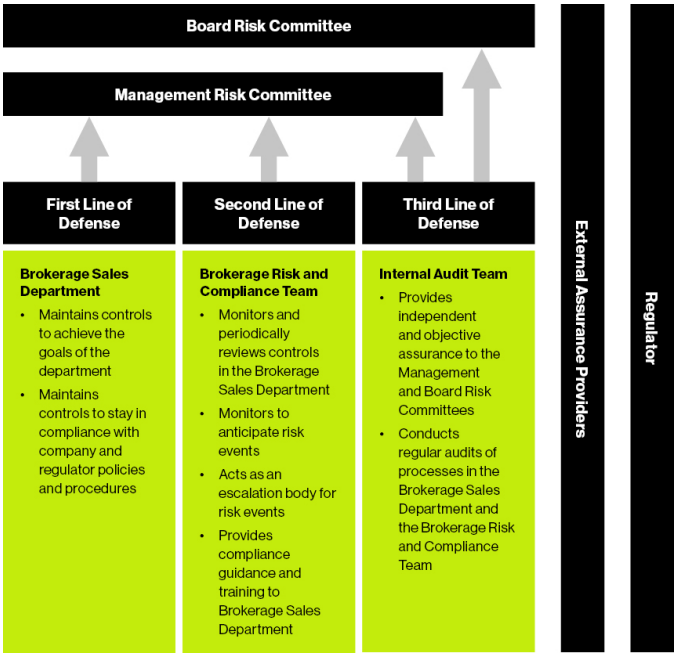

Fig. 1. Three Lines of Defense Against Information

- Information security events, which are increasing in frequency and expense, can have negative operational, financial, reputational, and strategic effects on the firm.
- Organizations frequently use frameworks like ISO/IEC 27001 and 27002, NIST Cyber Security Framework (CSF), Cybersecurity Capability Maturity Model [28], or HITRUST CSF [29] to enhance government mandates (CSF).

II. Information Risk Overview

The harm caused by risk occurrences can be reduced using information risk management. Since 2015, there has been an 8.2% decline in cybersecurity incidents for organizations that have implemented new technology and done evaluations to reduce cyber risk. Additionally, businesses who stop data breaches in their tracks within 30 days spend $1 million less than those that don't. [1]

This strategy places IT risk functions in a position to own, supervise, and work together on top risks. However, because most businesses have a separate information security department and few ERM teams have any IT specialists on staff, risk managers sometimes feel confused of their role in

managing complex IT and cybersecurity risks. By working together with the information security unit or senior leadership, progressive ERM teams assist information risk management initiatives. These ERM teams collaborate with top stakeholders to communicate IT risk appetite, provide status updates on information risk, and in certain cases, develop an enterprise-wide information risk framework.

III. Nomenclature

ERM must first comprehend the differences between fundamental information security concepts in order to effectively analyze the threat picture [2][3]. Information security refers to the protection of data and information systems against intentional and accidental interruption, alteration, and destruction by external or internal actors.

Information Technology risk is the possibility of unanticipated outcomes connected to the usage, ownership, and adoption of information technology. Examples include inadequate storage, IT services delivered over budget, inadequate business response, and inadequate or incompetent IT employees.

Information risk is the probability and effects of a threat to the integrity, confidentiality, and availability of information. Risks to the security of third parties, a lack of staff understanding, and inefficient incident response are all included. Information risk and IT risk overlap to some extent and include hazards including confidentiality breach, privacy violation, end-of-life support, and technological obsolescence. ERM generally can better frame the kinds of risks it confronts by understanding the crucial components considering the danger that information risk poses.

IV. Risk Determination

A better quantifiable parameter of risk would help to determine the risk of the system as a whole. Because every company is different, they all face different risks. You must first identify the hazards facing your company in order to create a plan of action to defend it. You can begin to estimate their likelihood of happening and the effects they might have on your organization once you are aware of those risks and gaps.

Because of this, the foundation of every cybersecurity policy is an information security risk assessment. Making choices based on risk for your firm requires having a clear understanding of the risks. Hence, understanding the likelihood and effect of a particular danger is crucial for the risk assessment process.

According to the standard outlined in NIST SP 800-53 [23], comprehension of the following topics is necessary for a meaningful risk assessment:

- Probability and effects of those threats successfully exploiting the vulnerabilities
- Possibilities for weaknesses within the organization
- Threats to the organization

$$Risk = (Threat \times Vulnerabilities) \times Impact \quad (1)$$

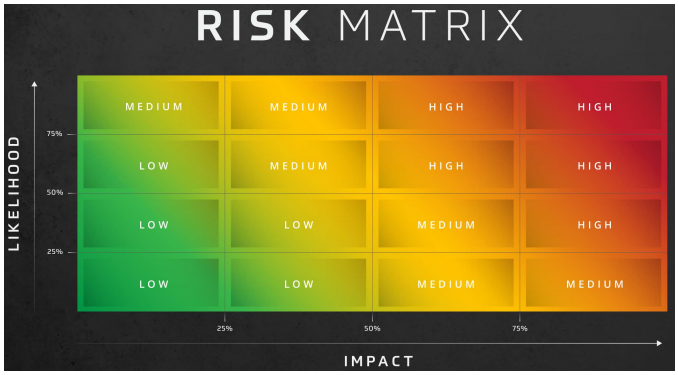

Fig. 2. Gauging Risk, An, M. F. (2007). Information Security Risk Assessment.

$$Risk = Likelihood \times Impact \quad (2)$$

Threats $\times$ Vulnerabilities, the first element of the calculation, determines the chance of a danger. For instance, if a company utilizes an outdated version of software that has a known security vulnerability, there is a risk that hackers would use that weakness to breach the business's system. But softwares are often updated by organization wherein the updates do include the patches and hence the threat is mitigated there and the weakness cannot be further exploited in that nature.

The factors of likelihood and impact actually generate a spectrum of residual risk rating namely: High, Medium, Low in that order to qualitatively quantify the risk. The residual risk assessment for any business may vary depending on the likelihood and consequences of each control weakness. That can be depicted in the Figure 2.

V. Threat and Mitigation of Information Risk

Investment experts rank cybersecurity as the biggest risk to a company's future growth [4]. Only 36% of boards claim to be adequately competent to assess and manage the organization's information risks, nevertheless. Even worse, just 4% of firms are satisfied that their risk landscape includes pertinent risks and that they have carefully analyzed how their current strategy would affect information security [5]. The intensity of occurrences is getting worse, which makes things more difficult. According to studies, enterprises will collectively spend more than $1 trillion on cybersecurity goods and services by 2021, and the entire cost of harm from information risk incidents will be $6 trillion each year [6]. Additionally, it is taking longer to identify those instances. Organizations now need more than 30 more days between 2015 and 2017, on average to find a potential information risk [7].

Last but not least, there are more events now than there were five years ago. Phishing and malware instances have climbed by about 23% [6]. Organizations frequently worry about information risk, thus ERM has to be aware of the elements that might make information risk worse.

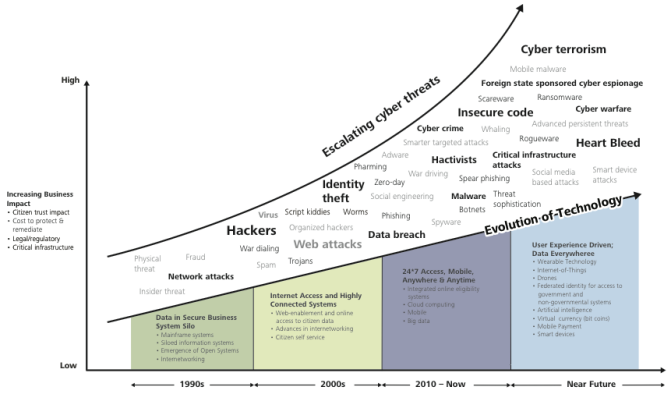

Fig. 3. Reproduced from the 2014 Deloitte-NASCIO Cybersecurity Study "State governments at risk: Time to move forward"

VI. Factors Impacting Information Risk

Four factors magnify the impact of information risk (see Figure 2) [8]:

1) Unsafe work practices by employees 70% of Chief Information Security Officers (CISOs) identified lack of candidates with matching skillset as the most likely factor contributing to a data breach at their organization [1].
2) Expanding the assault surface IoT connections will reach 25 billion by 2025, increasing the amount and diversity of connections that can be the target of assaults. [8].
3) Threats' growing sophistication — 12% of C-suite executives and IT executives said they are confident in their ability to recognize a sophisticated threat [5].
4) Third-party weaknesses — Sixty percent of CISOs are more worried in 2018 than they were in 2017 about a third-party data breach [1].

Risk management leaders must approach information security from all directions in order to be successful.

VII. Cause and Effect of Information Security Incidents

Information security incidents have many causes:

- A non-monitored third party, for instance, may have access to private client data that contain personally identifiable information.
- Employees that act insecurely could, for instance, submit their login credentials on a site that isn't secure or post them online.
- Immature governance structure - For instance, if a crisis occurs, the organization is more vulnerable because of unclear roles to play.
- For instance, the information security team depends on compliance or internal audit to assume responsibility of controls, which is poor security control hygiene.

The effects of information security events, however, are as wide-ranging. These dangers may have a strategic, operational, reputational, and financial impact on the firm:

- Strategic - Intellectual property theft or disclosure can put a strategic plan on hold or reduce competitive advantage.
- Reputational - The disclosure of customer personal data may lead to short-term revenue losses and long-term loss of investor and customer confidence.
- Operational - The company's ability to fulfill its contractual commitments is hampered by a denial of service assault.
- Financial - Important regulatory statutes must be followed in order to avoid severe financial penalties and onerous requests from regulators.

Risk managers and their organizations can spot a problem before it gets worse by understanding information security failure points and their results.

A. *Recent Information Risk incidents*

Information security events can result in bad media coverage that harms an organization's reputation in addition to the immediate harm to operations. The information security events listed below show the variety in severity and nature:

- When 150 million users of the company's MyFitnessPal app had their personal information exposed as a result of a data breach, a class action lawsuit was brought against Under Armour. [15][16].
- WannaCry ransomware, which impacted up to 19,000 patient appointments across 45 NHS institutions, was a victim of the National Health Service (NHS). [11][12].
- Attackers stole $100 million from each of Facebook and Google as part of a phishing campaign in which they pretended to be an electronics manufacturing partner.[13][14].
- The assault by the NotPetya virus on FedEx's TNT business hindered shipments and resulted in operational inefficiencies that cost the corporation $400 million in lost revenue and expenditures to repair technological systems. [9][10].

Leadership puts pressure on CISOs to keep breaches secret in order to prevent this reputational harm. In response, CISOs focus excessively on handling major security crises while ignoring standard incident response plans. The unnoticed issues that would have been discovered during normal inspections have the potential to turn into significant, crippling occurrences.

VIII. Frameworks

Information security risks may be managed in collaboration with IT and ERM. The IT department will handle the majority of the technical components, but ERM can increase its expertise with standard frameworks. Security risks are managed by IT risk frameworks which are as follows:

1) ISO/IEC 27001 and 27002
2) NIST Cyber Security Framework (CSF)
3) Cybersecurity Capability Maturity Model (C2M2)
4) HITRUST Cyber Security Framework (CSF)

A. *ISO/IEC 27001 and 27002*

These two frameworks were developed collaboratively by the International Electrotechnical Commission (IEC) and the International Organization for Standardization (ISO), and they were released in 2005. The frameworks are the most well-known and are designed to be used broadly across industries and different sizes of businesses. [17].

B. *NIST Cyber Security Framework (CSF)*

This optional framework may be used by businesses of all sizes and in all industries. Identification, protection, detection, response, and recovery from information security events are its five main tasks. Version 1.1, released in 2018, includes improved supply chain cybersecurity management and revised risk assessment [18].

C. *Cybersecurity Capability Maturity Model (C2M2)*

Although developed by the US Department of Energy, this model is applicable to all sizes, kinds, and industries of companies. In order to assess the organization's information security program maturity, it also comes with an additional toolbox that should be utilized in combination with the model itself.

D. *HITRUST Cyber Security Framework (CSF)*

The ISO/IEC 27001/27002 frameworks form the basis of the Health Information Trust Alliance. It is designed for enterprises managing personal health information and integrates requirements from federal healthcare legislation (PHI). In 2018, HITRUST gained NIST CSF certification, giving a way to ensure compliance with the goals of the NIST framework.

IX. Regulations and Compliance

Information security management goes beyond the organization. Globally, governments have implemented a number of regulations:

- POPI 2013: South Africa This extensive personal data protection rule guarantees that people can access their personal information, request the release of such information from a carrier, and specifies guidelines for the storage of personal information.
- Privacy Act 1989 (Amended 2014), Australia — This law controls when and how government entities can gather personal information. The people in charge of keeping the data safe must make sure that sufficient safeguards are in place to ensure that it is neither lost nor misused.
- US: 2015 Cybersecurity Act — This law specifies rules for the dissemination of knowledge about cybersecurity dangers. Organizations that share information with the government are subject to limited liability, and the government is free to share the information with other agencies at its discretion.
- General Data Protection Regulation (GDPR) — Businesses conducting business within the EU are required under GDPR to protect the personal information and privacy of EU individuals. The export of data beyond the union is also subject to regulation. The law stresses enforcement, establishes transparency rules, and permits the imposition of fines [21].
- EU: 2016 NIS Directive — The first information security law governing the entire EU was ratified in July 2016. Member countries have 21 months to put it into effect. Companies subject to this Act are required, among other requirements, to set security standards proportionate to the risks posed to the company. Additionally, the law grants the government the right to audit private businesses to verify compliance.

X. Cyber Risk Analysis on Equifax 2016 Data Breach

A. *Equifax Background*

It is vital to understand the Equifax and its functionality in the business sense as it helps to understand the risk parameters and its affects. One of the three biggest credit agencies, along with Transunion and Experian, is Equifax Ltd. It allows individuals to examine their credit report and allows companies to assess a customer's ability to manage their commercial affairs. [23].

B. *Breach Incident*

The online dispute system for Equifax has a known software vulnerability, according to a study by the Government Accountability Office (GAO) in March 2017 [30]. Attackers might get access to the Equifax system using this weakness. Down the line two months, the attackers started harvesting data including customers' Personally Identifiable Information (PII) using the Equifax vulnerability. The attackers employed strategies in order to maintain the stature of anonymity and surveillance the movements. The issue wasn't found until July 29, 2017, though. According to the GAO report, Equifax took the necessary precautions to remediate the issue and public this information to the victims. [24].

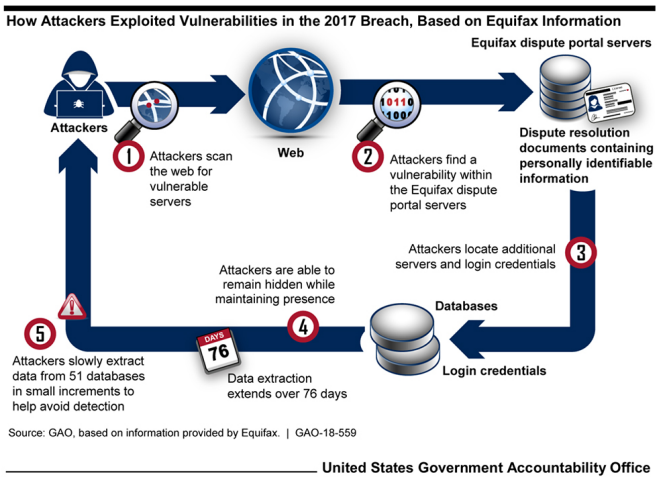

Fig. 4. Equifax Incident

C. *Impact*

There was a substantial impact on Equifax and its clients. Some of Equifax's relationships with the US federal government authorities were under threat. The Internal Revenue Service (IRS) reportedly intended to break its agreement with Equifax and work with a another provider, according to the GAO. When Equifax objected to this move, the IRS awarded it a short-term contract (United States Government Accountability Office, 2018). However, the IRS was successful in its argument to utilize Experian, a different credit reporting bureau, following further GAO inquiry.

D. *Risk Assessment*

In here, the assumed types of threat sources are as follows [25]:

- Adversaries (Hackers): Individuals, groups, organizations, or governments that aim to take advantage of the organization's reliance on cyber resources, such as electronic information, communications, and the capabilities that technologies offer for managing communications and information
- Accidental (Human Errors): Erroneous activities carried out by people while carrying out daily tasks
- Infrastructural: The failure of equipment, environmental controls, or software as a result of depletion of resources, age, or other events that go beyond standard operating norms.

Fig. 5. Widely followed Risk Management Process

*1) **Likelihood Assessment**:* The Figure 4 shows graphical representation of audited Likelihood of Threat Event in the Equifax breach.

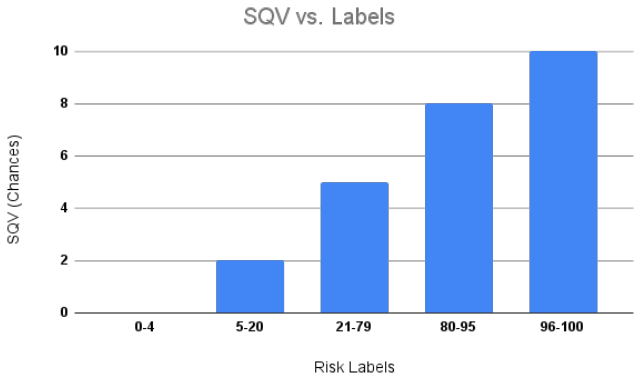

Fig. 6. Graphical Representation of Likelihood of Threat Event

In here, the SQV (Semi-Quantitative Values) which are decided according to the Risk Frameworks, the description of these qualitatively is done as follows:

- 96-100: Very High - The threat event will almost certainly be started by the adversary.
- 80-95: High - The threat event will highly likely be started by the adversary.
- 21-79: Moderate - The threat event will somewhat likely be started by the adversary.
- 5-20: Low - The threat event will unlikely be started by the adversary.
- 0-4: Very Low - The threat event will highly unlikely be started by the adversary.

*2) **Impact Assessment**:* The Figure 4 is almost as likely to depict the Impact of Threat Events. However, the description or more accurately, the very definition of such impacts would likely be changed in scenarios with SQV variance [26].

- 96-100: Very High - It is possible that the threat event will have a number of dire effects on organizational operations and organizational assets.
- 80-95: High - On organizational operations and organizational assets, the threat event may have a serious adverse effect. In here, the defined catastrophic adverse effect mean as follows:
  - Produce a significant loss in mission capability that is so great and long-lasting that the organization is unable to carry out one or more of its major duties
  - Cause significant harm to the organization's resources
  - Manifesting to a major financial deficit/loss
  - Results in severe or catastrophic harm to people, including fatalities or gravely injured lives.
- 21-79: Moderate - The threat event might be anticipated to significantly negatively impact organizational operations and organizational assets.
- 5-20: Low - On organizational operations and organizational assets, the danger event can be anticipated to have a little negative impact.

- 0-4: Very Low - On organizational operations, organizational assets, and persons as well as other organizations, it is possible to anticipate that the danger occurrence will have a small negative impact.

*3) **Risk Assessment Results**:* The final step would be to come up with the mitigation for these risks and the proposed mitigation techniques were as follows:

- Vulnerability: Apache Struts - The ASF also points out that projects that have already been deployed may be updated by simply replacing the JAR file in the WEB-INF/lib directory with the patched version of the commons - `fileupload` library. Most of the Maven based Struts were fixed by adding the following lines in the dependency [27]:

```
<groupId>commons-fileupload</groupId>
<artifactId>commons-fileupload</artifactId>
```

- Vulnerability: Default PIN - Advising users to make a complex password rather than a preset password and adding a layer of SHA-512 salt style encryption.

The final results of Risk Assessment on the Equifax breach were as follows:

Threat Events	Vulnerabilities	Impact	Likelihood	Risk
Apache Struts	Jakarta Parser Flaw	High	High	High
Default PIN	Culminating last four digits of SSN & DoB	High	High	High

XI. Conclusion

The ultimate objective is to reach a level of risk that the organization's management team finds acceptable considering all the scenarios of potential breaches and assigning value spectrum to assets. It's crucial to assess the risk in the organization environment and be aware of it so that a set of right policies can be enforced through mandatory mechanisms in order to reduce the likeliness of breaches and safeguard sensitive/critical data. Understanding the possibility and effect of any security threat are the two key components of risk assessment.

References

[1] Liu, Liyuan, et al. "Understanding data breach: A visualization aspect." International Conference on Wireless Algorithms, Systems, and Applications. Springer, Cham, 2018.

[2] Nieles, Michael, Kelley Dempsey, and Victoria Yan Pillitteri. "An introduction to information security." NIST special publication 800.12 (2017): 101.

[3] Kissoon, Tara. "Optimum spending on cybersecurity measures." Transforming Government: People, Process and Policy 14.3 (2020): 417-431.

[4] Arrow, Kenneth J., and Robert C. Lind. "Uncertainty and the evaluation of public investment decisions." Uncertainty in economics. Academic Press, 1978. 403-421.

[5] Linkov, Igor, and Alexander Kott. "Fundamental concepts of cyber resilience: Introduction and overview." Cyber resilience of systems and networks (2019): 1-25.

[6] Jacob, Johanna, et al. "Is the NICE cybersecurity workforce framework (NCWF) effective for a workforce comprised of interdisciplinary majors?." Proceedings of the International Conference on Scientific Computing (CSC). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2018.

[7] De Bruin, Rossouw, and S. H. Von Solms. "Cybersecurity Governance: How can we measure it?." 2016 IST-Africa Week Conference. IEEE, 2016.

[8] Suomalainen, Jani, et al. "Machine learning threatens 5G security." IEEE Access 8 (2020): 190822-190842.

[9] Alladi, Tejasvi, Vinay Chamola, and Sherali Zeadally. "Industrial control systems: Cyberattack trends and countermeasures." Computer Communications 155 (2020): 1-8.

[10] Kao, Da-Yu, and Shou-Ching Hsiao. "The dynamic analysis of WannaCry ransomware." 2018 20th International conference on advanced communication technology (ICACT). IEEE, 2018.

[11] Boddy, Aaron, et al. "A study into data analysis and visualisation to increase the cyber-resilience of healthcare infrastructures." Proceedings of the 1st International Conference on Internet of Things and Machine Learning. 2017.

[12] Ghafur, Saira, et al. "The challenges of cybersecurity in health care: the UK National Health Service as a case study." The Lancet Digital Health 1.1 (2019): e10-e12.

[13] Roberts, J. "Exclusive: Facebook and Google Were Victims of $100 M Payment Scam." Fortune Magazine (2017): 27.

[14] Chaulk, Kasey, and Tim Jones. "Online obsessive relational intrusion: Further concerns about Facebook." Journal of Family Violence 26.4 (2011): 245-254.

[15] Greve, Maike, Kristin Masuch, and Simon Trang. "The More, the Better? Compensation and Remorse as Data Breach Recovery Actions-An Experimental Scenario-based Investigation." Wirtschaftsinformatik (Zentrale Tracks). 2020.

[16] Hammouchi, Hicham, et al. "Digging deeper into data breaches: An exploratory data analysis of hacking breaches over time." Procedia Computer Science 151 (2019): 1004-1009.

[17] Nifakos, Sokratis, et al. "Influence of human factors on cyber security within healthcare organisations: A systematic review." Sensors 21.15 (2021): 5119.

[18] McCarthy, Charlie, and Kevin Harnett. National institute of standards and technology (nist) cybersecurity risk management framework applied to modern vehicles. No. DOT HS 812 073. United States. National Highway Traffic Safety Administration, 2014.

[19] Sun, Chih-Che, Adam Hahn, and Chen-Ching Liu. "Cyber security of a power grid: State-of-the-art." International Journal of Electrical Power & Energy Systems 99 (2018): 45-56.

[20] Kandasamy, Kamalanathan, et al. "IoT cyber risk: A holistic analysis of cyber risk assessment frameworks, risk vectors, and risk ranking process." EURASIP Journal on Information Security 2020.1 (2020): 1-18.

[21] Ouwerkerk, Eelco. "Beware of GDPR–Take your Cyber Risk Responsibility More Seriously." The InsurTech Book: The Insurance Technology Handbook for Investors, Entrepreneurs and FinTech Visionaries (2018): 175-178.

[22] Force, Joint Task. Security and privacy controls for information systems and organizations. No. NIST Special Publication (SP) 800-53 Rev. 5 (Draft). National Institute of Standards and Technology, 2017.

[23] Zou, Yixin, et al. "" I've Got Nothing to Lose": Consumers' Risk Perceptions and Protective Actions after the Equifax Data Breach." Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018). 2018.

[24] Wang, Ping, and Christopher Johnson. "Cybersecurity incident handling:

a case study of the Equifax data breach." Issues in Information Systems 19.3 (2018).

[25] Zou, Yixin, and Florian Schaub. "Concern But No Action: Consumers' Reactions to the Equifax Data Breach." Extended abstracts of the 2018 CHI conference on human factors in computing systems. 2018.

[26] UKEssays. (November 2018). Equifax Risk Assessment of Information Security. Retrieved from https://www.ukessays.com/essays/information-systems/equifax-risk-assessment-of-information-security.php?vref=1

[27] Luszcz, Jeff. "Apache struts 2: how technical and development gaps caused the equifax breach." Network Security 2018.1 (2018): 5-8.

[28] Barclay, Corlane. "Sustainable security advantage in a changing environment: The Cybersecurity Capability Maturity Model (CM 2)." Proceedings of the 2014 ITU kaleidoscope academic conference: Living in a converged world-Impossible without standards?. IEEE, 2014.

[29] Pandey, Atul, and Rinku Sharma. "Risk Management for Health Care Operations and Protected Healthcare Information." International Journal of Pharmacology and Biological Sciences 11.1 (2017): 55.

[30] Lyons, Angela C., Mitchell Rachlis, and Erik Scherpf. "What's in a score? Differences in consumers' credit knowledge using OLS and quantile regressions." Journal of Consumer Affairs 41.2 (2007): 223-249.