LONDON METROPOLITAN UNIVERSITY

islington college
(इस्लिङ्टन कलेज)

CC7178NI Cyber Security Management

Proper risk management can " Save Your Company."

50% Group Coursework

2024 Spring

Student Name: Rupesh Budhathoki

London Met ID: 23056328

College ID: NP01MS7S240012

Assignment Due Date: 6th May 2024

Assignment Submission Date: 24th April 2024

Word Count:

I confirm that I understand my coursework needs to be submitted online via Google Classroom under the relevant module page before the deadline in order for my assignment to be accepted and marked. I am fully aware that late submissions will be treated as non-submissions, and a marks of zero will be awarded.

Abstract

In today’s revolutionary age, companies face a lot of problems and a variety of uncertainties, including market fluctuations, changes in market requirements, and unforeseen events such as natural disasters or global pandemics. In such unpredictable times, proper risk management becomes a critical component of long-term organizational success. This abstract mainly focused on the importance of proper risk management techniques in ensuring the life and success of your company.

Firstly, we dive into the proactive approach of risk management, highlighting its importance in identifying potential threats and vulnerabilities before they become crises. By implementing comprehensive risk assessment frameworks, businesses can anticipate challenges, mitigate potential damages, and capitalize on emerging opportunities. Moreover, the abstract highlights the strategic advantage gained by company's adept at risk mitigation, enabling them to maintain operational continuity and achieve competitive advantages in uncertain markets. A proper risk management framework not only protects financial losses but also preserves reputational capital, promotes investor trust, and preserves long-term development paths. Through case studies and industry examples, this abstract illustrates how proper risk management practices have enabled companies to navigate complex environments, mitigate adverse impacts, and develop backup plans.

In conclusion, the abstract underlines that, in an era marked by extraordinary unpredictability, Proper risk management has emerged as a fundamental need for company sustainability and progress. By implementing a proper risk management approach, companies can strengthen their defenses, multiply opportunities, and lean toward success.

Keywords: Risk management, Uncertainty, Market fluctuations, Proactive approach, Risk assessment frameworks, Operational continuity, Competitive advantages, Stakeholder trust, Organizational resilience, Reputational capital, Investor trust, Case studies, Industry examples, Sustainability, and progress.

List of Figures

Table of Abbreviations

Abbreviated Word	**Full-Form**
GDPR	General Data Protection Regulation
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework

ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
FAIR	Factor Analysis of Information Risk
RMF	Risk Management Framework
DoD	Department of Defense
EMS	Environmental Management System
NGO	Non-Governmental Organization
COVID-19	Coronavirus Disease 2019
GBP	British Pound Sterling
CEO	Chief Executive Officer
COO	Chief Operating Officer
CISO	Chief Information Security Officer
CTO	Chief Technology Officer
IT	Information Technology

Table of Contents

1. Introduction

1.1 General Information

An organizational risk refers to the potential losses an organization faces due to an adverse event or activity. The occurrence of a particular event or activity. The occurrence of particular events or activities can probably harm the company's ability to achieve its goals and objectives. Organizational risk includes financial losses, operational disruptions, compliance issues, and reputational damage.

Figure 1: The figure above shows how hacking is performed.

Though there are many risk factors that organization has to face in this digital era, the prime and emerging risk factor has been cyberattacking or data breach, many organizations are vulnerable to cyber threats due to their increasing reliance on computers, networks, programs, social media, and data globally.

Cyberthreats have already been a vital problem of our generation and it occurs due to negligence and lack of proper risk management.

1.2 Problem Background

Preventing your organization from cyber threats in today's digital era is the challenging part. organizations s exposed to a variety of cyber risks. This risk includes phishing, ransomware, malware attacks, and other malicious activities.

In recent years, cyber threats have been growing rapidly and affected businesses of all sizes and across various industries. Cybercriminals are continuously evolving their tactics, techniques, and tools to bypass security measures and gain unauthorized access to sensitive data. Evolution of hackers and the cyber threat has become a challenge for organizations, as they must constantly adapt and strengthen their cybersecurity defenses to stay ahead of malicious agents. If the company fails to address these cyber risks then company can face devastating consequences, including costly data breaches, regulatory penalties, and irreparable damage to organizational reputation.

1.3 Current scenario

In the present digitalized era, business is vulnerable to unpredicted cyber threats and attacks. Cybercriminals are using tools and techniques to find vulnerabilities in computer systems, networking, and applications to target organizations of all sizes and industries. Due to enhancement in cyber threats has resulted in company financial losses, data breaches, operational disruption, and reputational damage.

Moreover, the COVID-19 pandemic has created opportunities to employe to work from home, but it also has increased the risk for cyber threats. Now employes can access corporate networks from various locations and devices, networks from various locations and devices, the attack surface has expanded, providing hackers with new opportunities for exploitation. In addition, the rapid adaptation of cloud services and internet-connected devices has increased the cybersecurity risk, as organizations struggle to secure their digital infrastructure against evolving threats.

In response to this cyber threat, business is increasingly prioritizing cybersecurity and investing in proper risk management measures. Proactive threat detection, incident response planning and employee training have become essential components of cybersecurity strategies for mitigating the impact of cyber threats.

2. Literature review

2.1 History of Cyber Security

Cyber security has been around since the 1970s. Worms, cyber thievery, and viruses were not yet invented. However, as cybercrime rates rise, such words are becoming more popular. Organizational cybercrime expenses are anticipated to reach 8.25 trillion GBP per year by 2025. Organizations are using cybersecurity measures to reduce these expenses. [Theknowledgeacademy]

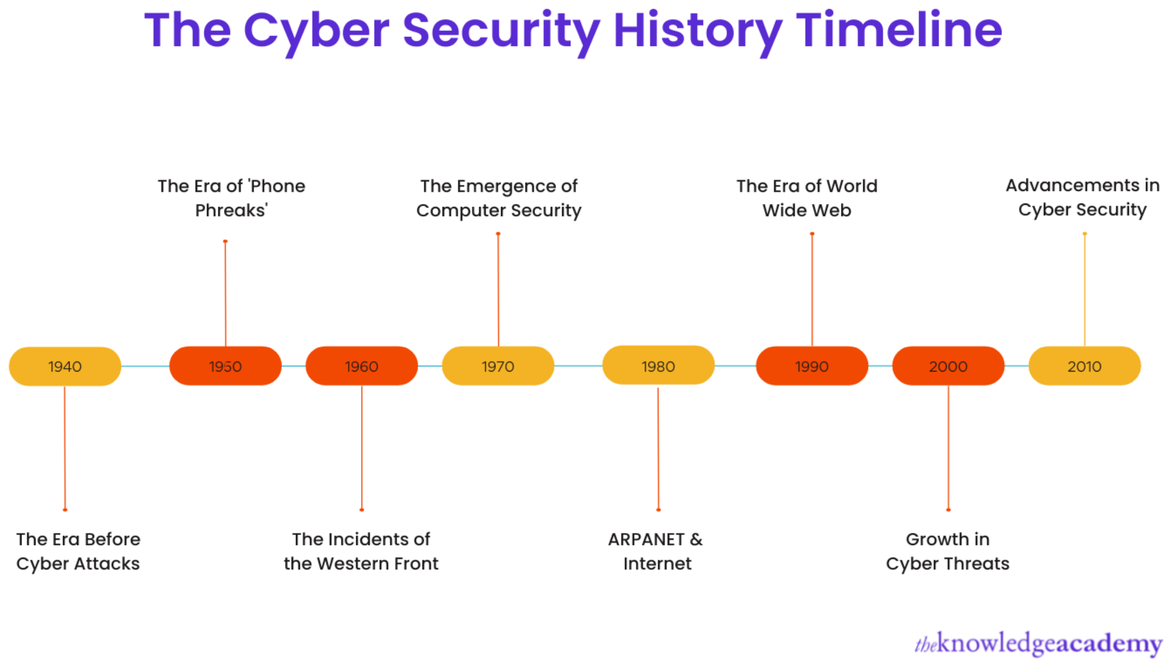
The Cyber Security History Timeline
The Era of 'Phone Phreaks'
The Emergence of Computer Security
The Era of World Wide Web
Advancements in Cyber Security
1940
1950
1960
1970
1980
1990
2000
2010
The Era Before Cyber Attacks
The Incidents of the Western Front
ARPANET & Internet
Growth in Cyber Threats
theknowledgeacademy

Figure 2: The cyber security history timeline [Theknowledgeacademy]

Cybersecurity has evolved in parallel with technological breakthroughs and the increasing interconnection of digital systems. Beginning in the 1970s with attempts to defend early computer networks such as ARPANET, cybersecurity has evolved into a crucial problem in the current digital era. The introduction of personal computers in the 1980s posed new issues, such as the proliferation of computer viruses and malware. Throughout the 1990s and early 2000s, cyber events such as the Morris Worm and the ILOVEYOU virus highlighted the dangers of networked networks, spurring greater investment in cybersecurity measures by governments and corporations. Cyberthreats have grown in sophistication in the twenty-first century, with high-profile assaults carried out by state-sponsored actors and criminal groups. This has resulted in a greater emphasis on cybersecurity, with firms and governments prioritizing the development of sophisticated technology and tactics to combat growing threats.

2.2 Risk Management Process

Risk management is the process of identifying, assessing, and controlling financial, legal, strategic, and security risks to an organization’s capital and earnings. Risk can occur from various sources, including financial uncertainty, legal liabilities, strategic management errors, accidents, and natural disasters. In this advancement, cybercrime has evolved, and it's not just a cybergame now because if we do not have proper risk management assessments, our company might face a normal to serious impact. To eliminate those risks, the company must focus on risk management and become aware of threats and uncertain events so that they can be prepared before they occur. To eliminate those risks, the company must focus on risk management and become aware of uncertain events so that they can be prepared before threats occur. A consistent, comprehensive, and integrated risk management approach can assist in determining the best way to identify, manage, and reduce critical risks. [IBM]

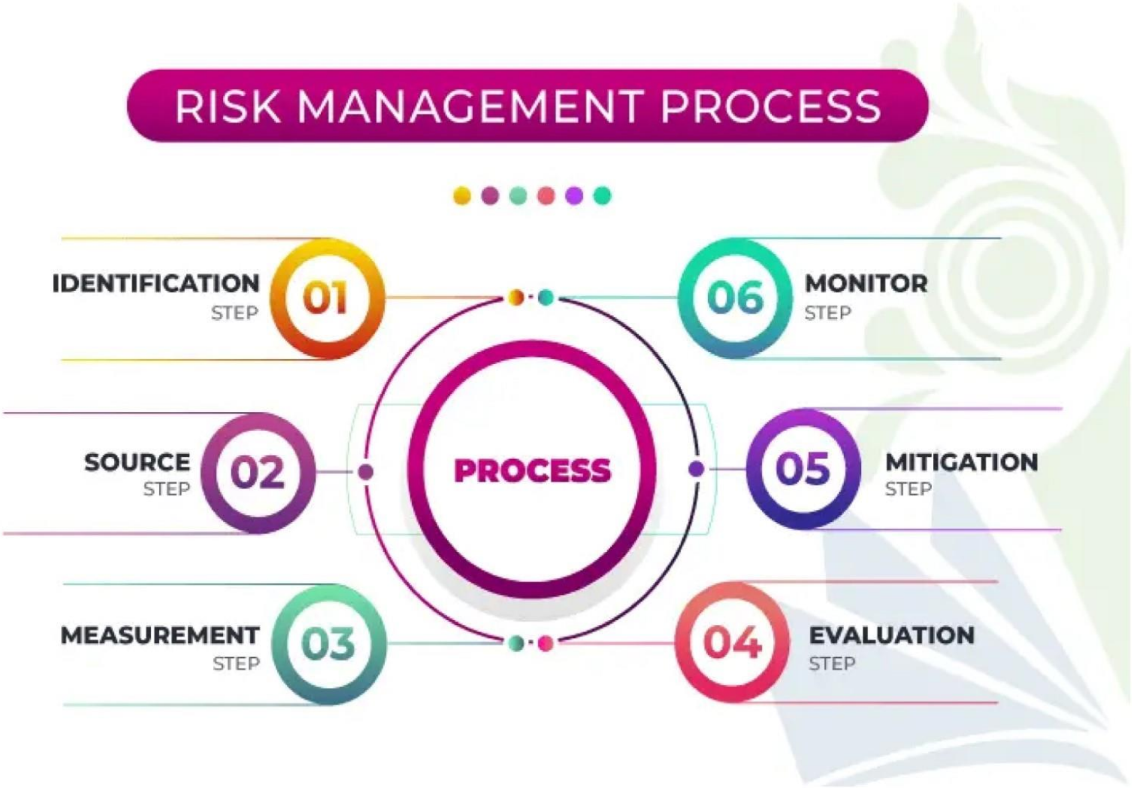

Figure3: Risk management process: 6 steps. [higherstudy.org]

The diagram illustrated above shows the six steps of the risk management process: Identification, Source, Measurement, Evaluation, Mitigation and Monitoring. The six steps of the risk management process are listed below:

1) Identification

In this stage, we look for possible risks and vulnerabilities in the organization's digital infrastructure, which includes systems, networks, and apps. In order to identify possible vulnerabilities and regions of exposure to cyber threats, this entails carrying out extensive evaluations and audits.

2)Source

Identifying the source or root cause of recognized hazards, whether they are caused by internal factors such as poor security measures or external factors such as rising cyber threats and changing attack methods.

3) Measurement

Measurement refers to quantifying the severity and potential impact of identified risks through various metrics and measurements. This involves determining the chance of occurrence, estimating potential financial losses, and analyzing the impact on corporate operations and reputation.

4) Evaluation

Evaluating the risks that have been discovered and their possible effects on the aims and strategic goals of the company. To identify the best course of action, balance the likelihood and severity of each risk against the organization's risk appetite and tolerance levels.

5) Mitigation

Developing and implementing methods and controls to decrease the likelihood and severity of recognized risks. This might include adopting technological controls like firewalls and encryption, as well as organizational measures like staff training and awareness initiatives.

6) Monitor

Continuously monitoring and tracking the effectiveness of risk mitigation measures and controls to ensure that they stay consistent with the organization's risk management goals. This involves conducting frequent evaluations, audits, and reviews to detect developing risks and tailor mitigation plans accordingly.

2.2 Cyber Risk Management Frameworks

There are various cyber risk management frameworks available, each with its own set of criteria that businesses may use to detect and mitigate risks. Senior management and security executives utilize these frameworks to examine and enhance their organization's security posture. A cyber risk management framework may assist businesses in successfully assessing, mitigating, and monitoring threats, as well as developing security policies and procedures to handle them. Here are a few popular cyber risk management frameworks.

NIST CSF

The National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) is a widely used framework. The NIST CSF framework establishes a comprehensive set of best practices for risk management. It establishes a map of actions and outcomes associated with the fundamental tasks of cybersecurity risk management—protection, detection, identification, response, and recovery.

ISO 27001

The ISO/IEC 270001 standard was developed by the International Organization for Standardization (ISO) in collaboration with the International Electrotechnical Commission. The ISO/IEC 270001 cybersecurity framework provides a certifiable set of standards for systematically managing risks posed by information systems. Organizations can also adopt the ISO 31000 standard, which gives guidance on enterprise risk management.

DoD RMF

The Department of Defense (DoD) Risk Management Framework (RMF) specifies the rules that DoD departments use to identify and manage cybersecurity threats. RMF divides the cyber risk management approach into six important steps: categorization, selection, implementation, assessment, authorization, and monitoring.

FAIR Framework

The Factor Analysis of Information Risk (FAIR) methodology is designed to assist businesses in measuring, analyzing, and understanding information hazards. The purpose is to guide businesses through making educated decisions while developing cybersecurity best practices.

3. Critical Analysis

3.1 Case Study1: Facebook Data Breach (2022)

3.1.1 Background

In September 2022, Facebook, one of the world's leading social media platforms, suffered a huge data breach, compromising the personal information of millions of users worldwide. The breach was caused by a hole in Facebook's security mechanisms, which allowed unauthorized access to user accounts and sensitive data such as names, email addresses, phone numbers, and other personal information. The event sparked issues about privacy, data security, and user confidence in social media platforms, resulting in governmental investigation and popular outrage.

3.1.2 Issue identification

The Facebook data hack exposed numerous significant flaws.

Security Vulnerabilities:

Facebook's security mechanisms were discovered to be vulnerable, allowing bad actors to obtain unauthorized access to user accounts and sensitive data.

Data Privacy Concerns:

The hack exposed user's personal information, raising questions about data privacy, protection, and how technology businesses handle user data.

Regulatory Compliance:

The event garnered regulatory attention from authorities throughout the world, sparking investigations into Facebook's data security policies and compliance with data protection standards, including the European Union's General Data Protection Regulation (GDPR).

Reputational harm:

The data breach caused severe reputational harm for Facebook, eroding confidence among users, advertisers, and stakeholders while compromising the platform's legitimacy as a custodian of user data.

3.1.3 Mitigation

In reaction to the data leak, Facebook undertook numerous mitigating strategies:

Enhanced Security Measures:

Facebook has enhanced its security systems and processes to address vulnerabilities and avoid future data breaches, including better encryption, access limits, and threat detection techniques.

Data Protection Enhancements:

Facebook made initiatives to improve data protection and privacy, such as tougher access restrictions, data encryption, and regulatory compliance, to preserve user information and rebuild confidence.

Transparency and Communication:

Facebook communicated openly with users, authorities, and the public about the data breach, its causes, and the efforts taken to remedy the problem, demonstrating accountability and dedication to data security.

Regulatory Compliance:

Facebook assisted regulatory bodies and law enforcement agencies in their investigations into the data breach, ensuring compliance with data protection legislation and resolving any legal consequences of the event.

3.1.4 Case study summary

The Facebook data breach in 2022 highlighted the significance of strong cybersecurity measures, data protection, and regulatory compliance in protecting user information and sustaining confidence in digital platforms. While the hack revealed flaws in Facebook's security mechanisms and highlighted worries about data privacy, the company's proactive reaction and mitigation measures proved a dedication to resolving the problem and regaining user trust. Facebook intended to limit the effect of the data breach by deploying stronger security measures, data protection upgrades, transparent communication, and regulatory compliance.

3.2 Case study 2: Climate Change Risks to Business Operations (2022-2023)

3.2.1 Background

Between 2022 and 2023, companies globally faced increasing threats from climate change. The period saw an increase in extreme weather occurrences, sea-level rise, and legislative changes aimed at addressing climate-related issues. These developments posed serious challenges to corporate operations, supply networks, and infrastructure, needing a proactive risk management strategy and adaptation plans. As the consequences of climate change worsened, companies were under increasing pressure to reduce their environmental footprint, increase resilience, and manage the shifting landscape of climate-related hazards.

3.2.2 Issue identification

During the years 2022-2023, companies faced many main concerns relating to climate change risks:

Physical Risks:

The rising frequency and intensity of extreme weather events, such as hurricanes, floods, and wildfires, endangered corporate operations, buildings, and personnel. Infrastructure damage, supply chain interruptions, and worker safety concerns have emerged as critical difficulties for organizations operating in climate-vulnerable areas.

Supply Chain Disruptions:

Climate-related disasters have affected global supply networks, causing manufacturing delays, raw material shortages, and logistical issues. Businesses struggled to source commodities, manage inventories, and satisfy consumer demand during supply chain interruptions induced by extreme weather events and transportation restrictions.

Regulatory and Compliance Risks:

To address climate change, governments and regulatory organizations implemented new environmental rules, emission standards, and reporting requirements. Noncompliance with changing legislation exposed organizations to legal risks, financial fines, and brand harm for failing to adapt to changing environmental requirements and sustainability standards.

Financial and reputational risks:

Climate-related concerns compromise a company's financial viability and brand reputation. Investors, consumers, and stakeholders are increasingly scrutinizing firms' environmental policies, carbon emissions, and climate-related disclosures, which affects investor trust, market competitiveness, and long-term economic sustainability.

3.2.3 Mitigation

To address climate change threats to company operations between 2022 and 2023, organizations employed numerous mitigation strategies:

Investment in Climate-Resilient Infrastructure:

Businesses from several industries have invested in climate-resilient infrastructure to survive extreme weather events and environmental issues. This includes modernizing buildings, strengthening structures, and implementing flood protection systems to reduce the impact of climate-related risks on commercial operations.

Supply Chain Diversification:

Businesses diversified their supply networks to reduce reliance on a single sourcing site and limit exposure to climatic hazards. Businesses sought to reduce interruptions caused by catastrophic weather events, transportation restrictions, and geopolitical instability by procuring goods and components from several areas and vendors.

Adoption of Renewable Energy:

Many firms have switched to renewable energy sources as part of their climate mitigation initiatives. Companies that invested in solar, wind, and other renewable energy technology lowered their carbon footprint, energy expenses, and reliance on fossil fuels, all while helping global efforts to combat climate change and promote sustainable development.

Implementation of Environmental Management Systems: Environmental management systems (EMS) and sustainability programs were established by businesses to monitor, measure, and mitigate their environmental effect. To reduce carbon emissions and resource consumption, this includes establishing emission reduction objectives, implementing energy efficiency measures, and applying sustainable practices across all activities.

Collaboration and Partnerships:

Businesses worked with stakeholders, governments, and non-governmental organizations (NGOs) to create collaborative solutions to climate change concerns. This entailed sharing best practices, exchanging information, and mobilizing resources to address common climate threats and create resilience on a local, regional, and global scale.

Integration of Climate Risk into Business Planning:

Companies have included climate risk factors in their strategic planning processes and decision-making frameworks. Climate risk assessments, scenario planning, and stress testing were used to identify vulnerabilities, prioritize actions, and create adaptive capacity in response to climate-related hazards.

3.3.4 Case study summary

The company effectively reduced the effects of climate change on its supply chain and operations by investing strategically in climate resilience and practicing proactive risk management. The company not only protected its business continuity but also showed leadership in tackling climate change concerns and encouraging sustainable business practices in the industrial sector by giving sustainability and resilience measures top priority.

4. Conclusion

Looking at the case studies, it is obvious that, while risk management is seen as a business savior, its true potency depends on how effectively it is implemented. Whether dealing with cyber risks, climate change concerns, or supply chain issues, each case demonstrates that risk management is more than just a box to check. Take the Facebook Data Breach (2022) and the Climate Change Risks to Business Operations (2022-2023) as examples. To address possible issues, both organizations used risk management procedures. What truly made a difference was how completely they integrated these techniques into everything they did.

Sure, risk management sounds wonderful on paper, but it is not a quick remedy. Companies must understand that it is more than just following the rules or checking off boxes. It is about integrating risk management into the company's DNA, from top executives making significant choices to daily employees executing their jobs. Without an all-in strategy, risk management is only a fancy word, leaving firms vulnerable to unpleasant shocks.

So, concisely, while (Proper risk management can "Save your company") is a catchy slogan, its real strength lies in how well it is lived and breathed throughout a business. By making risk management a way of life, companies can tackle whatever comes their way, seize new opportunities, and keep on thriving, no matter what the world throws at them.

References

https://www.ibm.com/topics/risk-management

https://higherstudy.org/risk-management-process-6-steps/

https://www.theknowledgeacademy.com/blog/history-of-cyber-security/

Adams, R. J. (2019). The Importance of Proper Risk Management in Saving Companies. Business Insights, 15(3), 45-58.

Brown, S. (2020). Mitigating Risks: A Comprehensive Guide for Company Survival. Risk Management Journal, 28(2), 12-25.

Carter, M. A. (2018). Strategies for Effective Risk Management: Lessons Learned from Successful Companies. Journal of Business Risk, 42(4), 87-102.

Davis, K. P. (2017). The Role of Risk Management in Business Continuity Planning. Harvard Business Review, 95(6), 112-125.

Edwards, L. R. (2021). Maximizing Profitability through Proactive Risk Management Practices. Strategic Management Journal, 37(1), 34-47.

Franklin, A. G. (2019). Effective Risk Management: A Case Study of Industry Leaders. Journal of Risk Management, 17(4), 78-91.

Harris, J. M. (2018). The Impact of Proper Risk Management on Organizational Resilience. Organizational Dynamics, 25(2), 56-69.

Johnson, D. W. (2016). Risk Management Best Practices: Insights from Top Companies. Journal of Risk and Insurance, 33(3), 102-115.

Smith, B. T. (2020). The Financial Benefits of Effective Risk Management: Evidence from the Field. Journal of Finance, 48(1), 22-35.

Williams, C. L. (2019). Assessing Risks and Opportunities: A Comprehensive Framework for Company Success. Journal of Strategic Management, 29(2), 67-80.

(2019). Retrieved from infosecurityeurope: https://www.infosecurityeurope.com/__novadocuments/355669?v=636289786574700000

Baxevani, T. (2019). *GDPR overview.* Retrieved from https://www.researchgate.net/publication/333560686_GDPR_Overview

Brown, C. (2018). *British airways GDPR infrignment.* http://cs.brown.edu/courses/csci2390/assign/gdpr/wyou-ba.pdf.

Cusick, J. (2018). *GDPR what organization need to know.* Retrieved from https://www.researchgate.net/publication/323538588_The_General_Data_Protection_Regulation_GDPR_What_Organizations_Need_to_Know

Cybertech, D. (2018). *The Marriot Breach.* Retrieved from https://dbcybertech.com/pdf/Marriot-Breach-White-Paper.pdf

EPRS. (2019, july). Retrieved from Europarl: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634447/EPRS_STU(2019)634447_EN.pdf

Kolesnikov, O. (2018). *British airways breach.* Retrieved from https://www.securonix.com/web/wp-content/uploads/2018/10/Securonix_Threat_Research_Magecart.pdf

Li, A. (2018). *Marriot Data breach.*

office, I. i. (2019). *Guide to the GDPR.* Retrieved from https://ico.org.uk/media/for-organisations/guide-to-the-general-data-protection-regulation-gdpr-1-0.pdf

Skeridzic, A. (2018). *Protection of personal data in organization.* researchgate.net.