Spring 2023

Current Cyber Security Challenges

Sriram Boppa

CURRENT CYBER SECURITY CHALLENGES

By

Sriram Boppa

B.S., SRM University, 2019

THESIS

Submitted in partial fulfillment of the requirements

For the Degree of Master of Science, With a Major in Information Technology

Governors State University

University Park, IL 60484

2023

Abstract

We have experienced exponential technical improvement during the last ten years. Cybersecurity issues are a result of the cyber world's increasing growth. Due to the way cybercriminals have adjusted their tactics to the new environment, there are now significant CS challenges.

More than 20 years later, the quantity and severity of cybercrimes have skyrocketed in just a few years as a result of previously unheard-of occurrences like the COVID-19 epidemic, contested elections, and rising geopolitical upheaval. Over time, it is likely that security risks will advance in sophistication and cost us more money: according to analysts, the worldwide cost of cybercrime will rise from $3 trillion in 2015 to $10.5 trillion in 2025, a 15% increase.

The secret to averting a CS assault is proactive protection. Discover the top CS risks that, according to experts, the globe will face in 2022, along with what you can do to prevent yourself and your company from becoming a target.

As a result, the sector is seeing an increase in demand for specialists who can decisively address security issues, creating the foundation for a safer cyberspace. If you are interested in developing a career in this field, you might think about checking out these CS courses. You could also look at the premium selection of CS courses.

Table of Contents

Abstract 2
Introduction 4
Objectives 5
Literature Review 5
Research Framework 13
Future Research Agenda 18
Conclusion 18
References 19

Introduction

Almost 95% of information is transported via the internet, making it one of the newest technologies that is always developing. Nevertheless, only a small percentage of recipients can be certain that the information they get has not been altered by a third party or that it is secure. We are all aware that developers and programmers constantly work to create algorithms, software, data encryption applications, and a variety of other tools to enable users to send data securely. However, hackers, attackers, and other third parties constantly try to alter or decrypt data by taking advantage of vulnerabilities in our systems, applications, business networks, and other areas.

As per (Preethiga Narasimman 2023) the practice of preventing malicious assaults on networks, computers, servers, mobile devices, electronic systems, and data is known as cybersecurity (CS). It is also known as electronic information security or information technology security. The expression, which is used in a variety of contexts, including business and mobile computing, can be categorized into a few basic groups, including

- Network Protection
- Privacy and Data integrity
- Operational Security.

With the widespread adoption of information and communication technology, CS has received more focus lately. especially at this time, when most economies are progressively recovering from the recent COVID-19 pandemic and permitting admission to completely immunized visitors into their respective nations. Organizations are under a lot of strain, and policymakers are progressively adjusting to the present landscape of information-related security threats (Arun P.C Sukumar al.2019).

The extreme losses resulting from CS abnormalities are well recorded, spanning the globe from the United States to Japan, Canada to South Africa, China to the United Kingdom. For instance, businesses in the United Kingdom suffered losses from hacking of about $35 billion in 2016 (Samarati, M, 2017).

Objectives

In this study, operational-level analyses of current CS risks are combined with investigations of countermeasures.

This paper's goals are:

1. Identify and evaluate contemporary CS threats.
2. Identify the most practical tactical methods for reducing these threats.

Literature Review

Digital transformation and technological progress have created significant safety challenges. Utilizing these patterns, hackers, assailants, and cybercriminals scour an organization's information technology system for openings and weaknesses. During the Covid19 pandemic, Trend Micro Research (https://www.sba.gov/managing-business/cybersecurity)conducted a study that came to the conclusion that there were more than 910k spam messages, 737 malware attacks, and 48,000 views on suspect links globally up until the beginning of April 2020. Additionally, there was a 260% increase in malicious URLs and a 220% increase in spam emails between February 2020 and March 2020. Detecting spam and malware is primarily targeted at the United States. The top 10 cybercrime risks during the COVID-19 pandemic are shown in Figure 1 below.

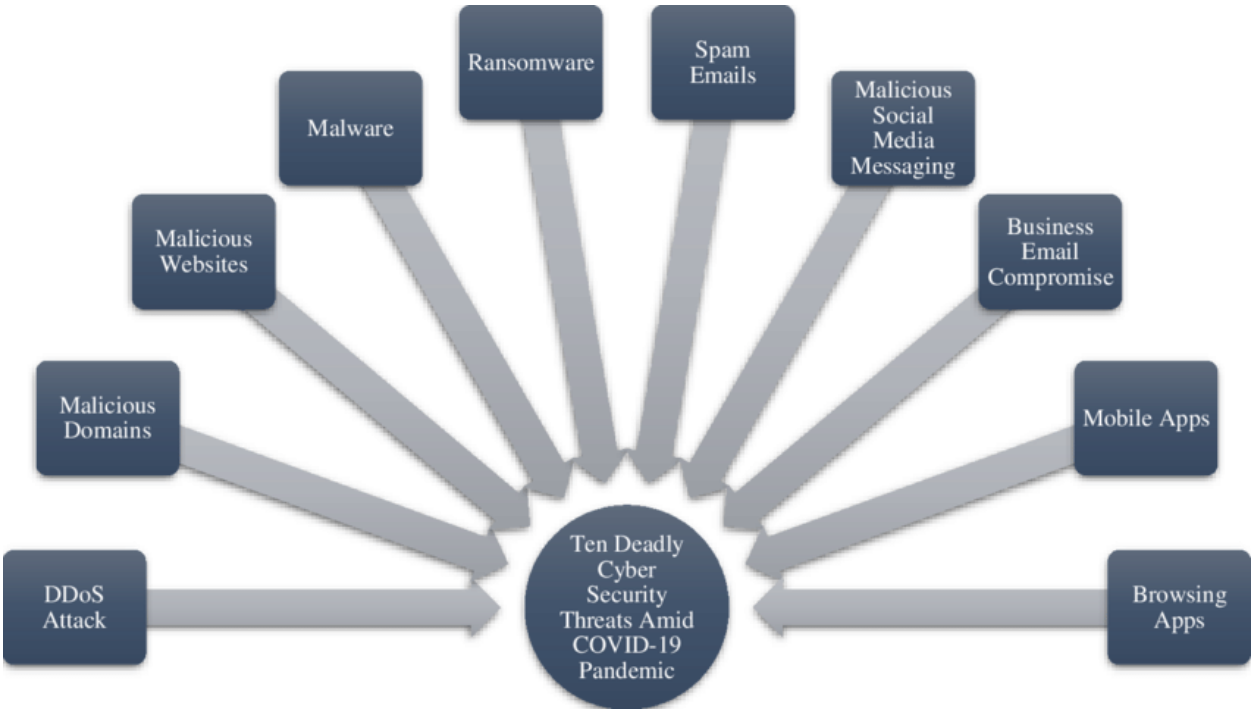


Figure 1: Top 10 Cybersecurity Threats Amid COVID-19

2023's New Cybersecurity Challenges and Solutions (Preethiga Narasimman 18th March 2023)

Adapting to a Remote Workforce

One of the most prevalent security concerns for employees when working from home is identity theft. Due to neglect, exhaustion, or ignorance, employees may unintentionally provide hackers access to their computers or corporate files. The main problem in CS will always be protecting remote and hybrid work settings.

Cloud-based CS solutions that safeguard the user's identity, device, and cloud are essential for secure remote working.

Applications of the Future 5G

The features of 5G networks increase the threat to CS. The nation's citizens, businesses, and communities trying to implement 5G are ill-prepared to assess and manage its risks.

Finding the names of third-party attackers engaged in a continual process of illegally accessing customers' data and abusing their privacy and faith in the companies they are working with is essential as a solution.

Attack With Blockchain and Cryptocurrency

Blockchain-based systems are susceptible to assaults from both insiders and outsiders. Many of these assaults made use of well-known strategies including phishing, social engineering, data interception, and code faults.

To protect businesses from cyberattacks, more durable technological infrastructure may be created using blockchain-powered CS controls and standards. It may also be required to combine Blockchain with other cutting-edge technologies like AI, IoT, and ML.

Ransomware Development

Ransomware is a type of malware that encrypts files on a victim's computer and holds them hostage until a ransom is paid. In the past, organizations could keep their data fairly secure by following a standard backup routine. Without paying the ransom, the organization might be able to retrieve the hostage data, but it wouldn't necessarily stop the bad guys from trying to get the information.

Customers should thus focus on frequently backing up their devices, using the most latest anti-malware and anti-phishing tools, and maintaining constant device updates.

IoT Attacks

IoT attacks are cyberattacks that use any IoT device to get access to private customer data. Attackers frequently destroy a device, install malware on it, or get access to further company information.

One needs to do thorough security analyses and maintain communication protection techniques like encryption to implement the increased security of IoT devices.

Cloud Attacks

Using their cloud infrastructure to deliver hosting, computing, or storage services, remote service providers are the target of a cyberattack. Examples of this include assaults against service platforms using the SaaS, IaaS, and PaaS service delivery paradigms.

By being aware of the principles of cloud security and some of its most pervasive weaknesses, we may lessen our chances of becoming a victim of cyberattacks.

Spear-Phishing Attacks and Phishing

In this type of email attack, the attacker poses as a representative of an important, respected business in order to get sensitive information from customers through deceptive electronic contact. A spear phishing email assault targets a specific individual or company.

Utilizing anti-phishing technologies like antivirus software and an anti-phishing toolbar, sandboxing email attachments, and educating staff are a few ways to combat phishing and spear-phishing assaults.

Software vulnerabilities

Software vulnerabilities are defects in the code that might provide an attacker access to a system. These mistakes in the software's code or design might be the cause of these issues.

Software with vulnerability management capabilities has a CS plan. In order to reduce the possibility of further security breaches, it actively searches the network for vulnerabilities, detects them, and provides suggestions on how to fix them.

AI and machine learning attacks

The best way to deal with software vulnerabilities is to prevent them from ever happening. Secure coding practices must be learned by software developers, and automatic security testing must be used throughout the whole software development cycle.

BYOD Guidelines

Personal devices, which are less secure and more likely to contain security issues than corporate ones, are more likely to be used to infiltrate business networks, whether or not BYOD are approved by IT. Therefore, BYOD security must be understood and addressed by businesses of all sizes.

One of the management options includes services for BYOD, and the procedure starts with an enrollment app that connects a device to the network. Company-owned devices can be set up either individually or in bulk.

Insider Threats

These entail a current or former employee or professional friend gaining illegal access to a system within an enterprise. They are difficult to locate, difficult to stop, and laborious to clean up.

However, you may reduce the risk of insider assaults by combining stringent guidelines and astutely used technology.

Outdated equipment

The serious security risk presented by outdated equipment may go unnoticed by many businesses. Businesses that delay equipment upgrades due to the higher expense may wind up spending more money than required to recover from a cyberattack. Security breaches can cost a company money, damage its reputation, and cause a drop in sales in addition to being expensive in and of itself.

Even while upgrading hardware might be expensive, the financial costs to your business of utilizing out-of-date software are too great to be ignored. It is also crucial for preventing cybercrime.

Serverless Apps Security Issue

Serverless computing's event-driven structure and absence of permanent states are drawbacks for certain developers. Because local variables' values don't remain true between instantiations, developers that need persistent data may encounter problems.

Employing the help of your company's CS experts may be the best line of action for people who use serverless architectures.

Attacks on the Supply Chain are Increasing

When someone breaches your digital infrastructure by employing an outside partner or supplier who has access to your data and systems, this is known as a supply chain assault.

Upkeep and maintenance of a highly secure build infrastructure, prompt application of OS and software security upgrades, and creation of secure software updates as part of the software development lifecycle.

Rising Numbers of Mobile Malware

As the global mobile markets are being attacked, attackers are concentrating increasingly on smartphones and tablets, which has resulted in a surge in mobile malware.

Implementing a formal Bring Your Own Device (BYOD) or Enterprise Mobility Management (EMM) framework is typically one of the greatest business initiatives.

Attacks on APIs

An API attack is the unlawful or unauthorized usage of an API by automated threats, such as access violations, bot attacks, or abuse. An API attack may result in massive data losses, the theft of personal information, and service interruptions.

Organizations can encourage the usage of push notifications, employ two-factor authentication, and encrypt the data to defend against attacks on API.

Cyber experts are concerned about a new wave of drone theft.

Drones are becoming a bigger worry for police who are in charge of both law enforcement and company protection. Law enforcement agencies and aviation authorities are becoming increasingly concerned about the hazards posed by drones.

Fortunately, there are several methods to make any drone more secure against the possibility of drone hacking. The drone's firmware must be updated on a regular basis.

Increase in hacktivism

Hacktivists engage in damaging or disruptive behavior to further a cause, whether it be political, social, or spiritual. These individuals or groups commonly identify as "virtual vigilantes," attempting to expose dishonesty, wrongdoing, or corporate greed, promote awareness of violations of human rights, oppose censorship, or call attention to various types of social injustice.

One of the ways to combat hacktivism is to have a detailed plan.

- Establishing a reaction strategy
- Vulnerabilities should be checked
- Enhancing the security apparatus
- Monitoring social media to learn about the stated goals of hacktivists

Measures To Prevent Social Engineering

Cybercriminals effectively manipulate their targets' mentality using social engineering to obtain crucial information from them. Users are more likely to make security mistakes and steal sensitive data, like banking passwords, login credentials, system access, and other similar data.

Cyberattacks should be avoided by organizations using technology and training. You must adopt an integrated approach, including multi-factor identification, email gateways, reliable antivirus software, staff training, and others, to prevent such social engineering assaults because there is no one-stop solution to combat these social engineers.

Security of Hybrid and Remote Workforces

To enable safe access to programs for both on-premises and remote workers, a thorough study of access strategies is necessary, especially for remote users. Hybrid work has the same challenges as remote work, including the lack of a network border, the need to provide access from a variety of devices, and the demand to protect on-premises equipment.

A few strategies for protecting remote employees and their applications include identifying shadow IT, reducing risk via URL and web category filtering, installing virus protection, and creating data loss prevention (DLP).

Weaponization of firmware attacks

The number of firmware vulnerabilities has roughly grown five-fold over the previous three years according to the NIST National Vulnerability Database, making it one of the most serious problems and difficulties in terms of CS. Mobile and remote employees who utilize unsecured networks and personal devices run the risk of being particularly exposed.

You should take precautions to ensure that you're constantly avoiding plugging in USB devices you don't recognize, purchasing equipment with additional firmware security layers, keeping current PCs as current as feasible.

Deep Fake Technology

Deep fake dangers fall within the categories of traditional CS, law, society, and the individual. Two approaches have often been put up to deal with the problems brought on by deep fakes: either utilize technology to spot fake videos or promote media literacy.

Research Framework

The significance of a strategy plan for mitigating against malevolent threats or players cannot be overstated. An organizational security strategy should be meticulously drafted as the first line of defense against the majority of CS threats. Security policies are described by (S. P. Berman and J. W. Gately 2020) as clear instructions that serve as a guide for employee behavior with regard to information protection. They are also fundamental building blocks in the creation of effective controls to ward off potential security threats, and this can only be implemented by providing employees with training using clearly stated policies and procedures.

Mitigation Methods

When it comes to preventing harmful threats or actors, the value of a strategic plan cannot be overstated. Carefully drafting an organizational security policy is the first step in protecting against the majority of CS risks. (S. P. Berman and J. W. Gately, (2020)) Security policies are defined as clear instructions that serve as a guide for employee behavior with regard to protecting information. They also serve as fundamental building blocks for the creation of effective controls to ward off potential security threats. Security policies can only be put into practice by providing employees with training and well-articulated policies and procedures.

One simple issue drives all security efforts: How can you allow the right people access to the right systems for the right period of time while keeping the wrong people out? (TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020). Some crucial actions must be made in order to significantly lower the danger of remote unauthorized access for organizations:

1. Identity and access control
2. Vulnerability management (exposure to technology)
3. Risk from third- and fourth-parties
4. Security for Email
5. Web Security

A strong approach will contain the following to protect against these dangers, notably phishing and web-based attacks:

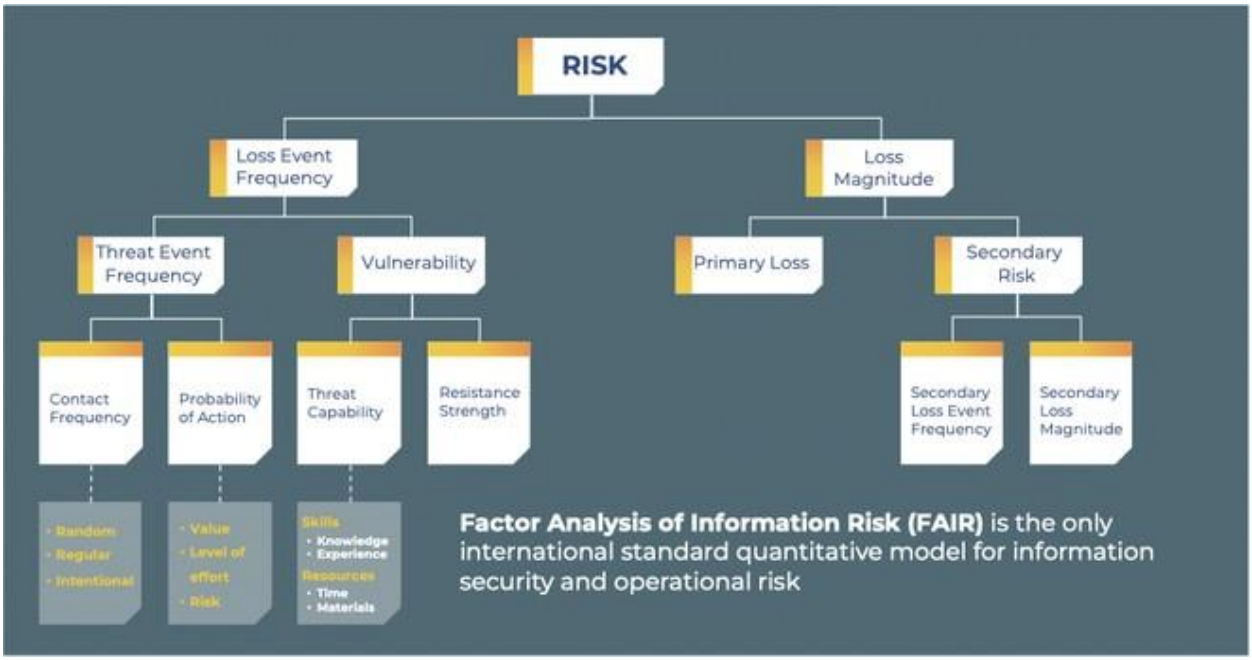
a) Server hardening

b) Continuous infrastructure awareness
c) Aggressive threat hunting

Although multi-factor authentication has improved, passwords are still often used as a form of authentication. Process hardening will be greatly aided by advancements in biometric validation, including identification based on retina scan, fingerprint, etc. (TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020) (Levi Gundert (2020)) supports the significance of threat intelligence and demonstrates how a business may actively gather this information from the open, deep, and dark web in order to better comprehend the degree of exploitation of vulnerabilities and assess the associated risk. Threat intelligence encourages firms to recognize the strategies, tactics, and procedures used by adversaries and determine whether these fresh approaches may render the current security controls ineffective (TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020). Every firm should do a comprehensive IT asset management inventory, according to (Levi Gundert (2020)), which offers an intriguing viewpoint and may assist determine which assets are vulnerable or which assets would have a significant negative effect on the business. Hardening fundamental security controls is a good place to start when implementing mitigation strategies (TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020). The entire security posture of a business will be strengthened by addressing issues with password complexity and storage needs. Organizations may detect particular vulnerabilities that pose real risks with vulnerability intelligence tools, which also provide visibility into the likelihood of exploitation. (Levi Gundert (2020)). A contextual study on the effective use of threat insight is providing threat expert anticipatory guidance of upcoming attacks linked to threat vectors. Sources like underground networks, glue locations, and debates might provide an association with crucial information. The examiner can then collaborate with other security teams to address significant holes, increase focus framework testing, and improve security control in order to stop the planned attack. (Levi Gundert (2020)) . (Levi Gundert (2020)) claims that risk modeling gives a tool to evaluate present risks critically and predict measurable financial rewards in CS. When attempting to evaluate their risk profile, organizations must take into account the general security of their partners, suppliers, and other third parties.

FAIR Risk Model

A company can develop a quantitative risk evaluation model with the FAIR Risk Model that includes precise odds for loss due to precise categories of threats. The FAIR Risk Model is graphically depicted in the figure below.



Source 1 https://www.fairinstitute.org/blog/fair-model-on-a-page

Figure 2 THE FAIR Framework, with elements informed by intelligence highlighted

This quantitative approach focuses on comprehending, analyzing, and quantifying data risk in genuinely monetary terms for information security and functional risk. An organization can create risk models using the FAIR model that (Levi Gundert (2020)):

a) Display precise loss odds in monetary terms.
b) Are more open about assumptions, factors, and results.
c) Calculate a specific risk assessment.

Starter Pack for SMB Protection

But how can a company defend itself, what are the fundamental measures they can take without spending a lot of money on threat intelligence, vulnerability information, and risk modeling?

According to (Kevin D. Mitnick, William L. Simon, (2002)), every employee should have the necessary training to adhere to fundamental standards like:

- Be wary of web connects and email connections.
- Keep your PC for business, your phone, and your records separate.
- Be incredibly thoughtful when it comes to the people you work with and are around.
- Avoid connecting personal or unauthorized storage devices or equipment to your computer, cell phone, or organization.
- Exercise caution when downloading programs.
- Don't provide personal or commercial information.
- Be vigilant for intrusive pop-ups
- Use secure passwords, and
- conduct online transactions more securely.

There are many technological solutions that can assist lower risk, but CS defense is fundamentally about people (TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020). The greatest asset and the biggest threat to any corporation are its employees. It is impossible to overestimate the importance of hiring talented security specialists, but as an organization, there are several concepts that must be ingrained in those who manage CS prevention and rehabilitation. The three P's (positivity, patience, persistence) and the three E's (execution, empathy, emotional intelligence), as well as the three C's (curiosity, creativity, and communication), were named by (TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020).

A thorough list of the top ten methods used by small companies to secure their information is occasionally published by the United States Small Business Administration (SBA). These contain (US Department of Défense (2021)):

- Guard against malicious software, malware, and viruses.
- Protect networks by utilizing a firewall and encryption
- Create a detailed arrangement of safety procedures and methods
- Train staff members on best practices;
- Mandate that all customers use very strong passwords.

- Adopt best practices for prepaid cards.
- Establish a reinforcement system that is accepted and strictly adhered to
- Control real access to data assets

Prevent Phishing Attacks

Safeguard all websites How can phishing scams be avoided? In line with (Levi Gundert (2020))

1) Being aware is essential. Avoid clicking on links or files, and look out for warning signs.
2) Use a reliable spam filter, but understand that it won't capture everything.
3) Use domain-based message authentication, reporting, and conformance (DMARC), Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and authentication checking.
4) Steer clear of sending private information.
5) Check any dubious requests.
6) Create unique, strong passwords; never reuse them.

Future Research Agenda

Ways of Mitigation When it comes to preventing malicious attacks or players, the value of a strategy plan cannot be overstated. The meticulous drafting of an organizational security strategy is the first stage in protecting against the majority of CS threats. Security policies, according to (S. P. Berman and J. W. Gately 2020), are unambiguous directives that outline how employees should behave in terms of protecting information. They also serve as the fundamental building blocks for the creation of effective controls to ward off potential security threats. Security policies can only be put into practice by providing employees with training and well-articulated policies and procedures.

Conclusion

The most valuable assets of an organization, its data, people, and technology assets, are constantly under attack by malicious players who are constantly evolving CS dangers. CS danger identification and prevention is a dynamic process that calls for ongoing training and evaluations. A risk-centric strategy forces organizations to follow stringent guidelines and objectives. CS The overall security strategy must specify goals and disseminate them throughout the company. The objectives set must be clear, quantifiable, and doable in order for security engineers and architects to be free to make adjustments as required and for results to be readily apparent. In a field where threat actors' methods, tactics, and processes are continuously changing, it can be extremely fatal. Although risk cannot be completely eradicated, it is possible to assess it and ensure worthwhile benefits for any organization that employs such practices by carefully applying the steps in this study.

References

https://www.sba.gov/managing-business/cybersecurity

https://www.knowledgehut.com/blog/security/cyber-security-challenges

https://www.studocu.com/in/document/i-k-gujral-punjab-technical-university/mech/cyber-security/7108006

Arun P.C Sukumar, Zimu Xu, Krishna Satyanarayana, Richard Tomlins (2019) "An exploration of cyber-security risk management in small businesses: The case UK Micro and Small firms" ISBE 2019 Conference Proceedings, Institute for Small Business and Entrepreneurship, ISBN 978 -1-900862- 32-5. pp 1.

Samarati, M, (2017), Cybercrime cost UK businesses £29 billion in 2016, IT Governance Institute, [Online] Accessed 2nd March at https://www.itgovernance.co.uk/blog/2016-cybersecurity-breaches-cost-uk-businesses-almost-30-billion/

S. P. Berman and J. W. Gately, (2020) "COVID-19 and Its Impact on Data Privacy and Security,".[Online].Available:https://www.lexology.com/library/detail.aspx?g=dec8ccabd74a4bc1-9e4a-9b1e5626e936.[Accessed: 04-May-2020]

Levi Gundert (2020) The Risk Business, What CISO Need to Know about Risk-Based Cybersecurity. Permission Department, CyberEdge Group, 1997 Annapolis Exchange Parkway, Suite 300, Annapolis, MD, 21401, ISBN 978-1- 948939-16-4 (eBook). pp 3 -93

Khan, Navid & Brohi, Sarfraz & Zaman, Noor. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic. 10.36227/techrxiv. 12278792.v1.

Kevin D. Mitnick, William L. Simon, (2002) The Art of Deception, forwarded by Steve Wozniak. Wiley Publishing, Inc. 10475 Crosspoint Blvd., Indianapolis, IN 46256. ISBN: 978-0-7645-4280-0, Chapter 12, pp 260.

TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercri%20meand-digital-threats/coronavirus-used-in-pam-malware-file-%20names-%20and-malicious-domains [Accessed: 04-May-2020]

US Department of Defense (2021)
https://www.defense.gov/News/Releases/Release/Article/2833%20006/strategic-direction-for-cybersecurity-maturity-m/