Review

Data Protection in Organization by the Implementation of Cyber Security

Syed Adnan Jawaid

University of Maryland-College Park, MD 20742, United States; Email: adnan.jawaid@hotmail.com

ABSTRACT: ***Background***: Cyber security is used to save the important data from getting hacked, took by some unknown access. It makes our environment a safe place for us to work out or share our information and since privacy is almost everyone's top priority, there must be the surety of saving the private information. **Methods:** In today's world cyber security is really important as there are now many devices, websites, new technology which makes it a lot easier for hackers to get into anyone's files which stores crucial data. However, many steps can be reserved to protect the data such as; educating your employees with how to prevent your files or computers from getting hacked, avoid clicking on websites that don't seem safe, use firewalls, antimalware system and most importantly make sure to keep passwords that are hard to guess and try to go for a face recognition instead of pins and passcodes. **Results and Conclusion:** This all does not only makes using technology safe but also favors your business for the safety of employees working within the organization. The customers being assured about their data being safe, improves productivity since viruses can slow down computers which may trigger the focus of staff during the working hours. It could save your system from adware; the links of websites are also prevented from slow internet speeds. There is no denying at the fact that cyber security is a major requirement for everyone who is indulged with technology today.

Keywords: Cyber security; privacy; awareness; impact; cyber-attacks; benefits of cyber security.

1. INTRODUCTION:

1.1. Cyber Security Protects Data

Cyber security safeguards data, networks, programmes, and other information from unauthorized or unsupervised access, destruction, or change. Because of various security concerns and cyber-attacks, cyber security is crucial in today's environment. Many businesses create software for data protection. Cyber security is crucial since it protects not only our systems from virus attacks but also helps to secure information [1].

With the widespread usage of electronic devices today, everyone needs to have appropriate cyber security. It guarantees the security of our personal information, sensitive data, personally identifiable information, protected health information, official documents, and governmental and commercial information systems. Without Cyber Security, anyone can steal, abuse, and misuse our data without our consent.

It is crucial for all users of electronic devices who often and routinely use them to keep their data and vital documents secure. Cyber security has a significant impact on young people's mental health. It has consistently been the main source of annoyance, sadness, rage, and uncertainty. There are numerous methods for providing cyber security, including antivirus, antimalware, end-user protection, etc. To prevent unwanted access to data centers and other electronic systems, both individuals and businesses employ this. It is advised that cyber security foundations be strengthened in order to better protect sensitive data, ID systems, and private information.

The right to privacy is seen as a basic human right and is legally protected. This used to indicate that people should be free to live their lives inside the confines of their own homes without the interference of the government. Today, having a private life entails being allowed to interact openly, make unrestricted decisions, and conduct online searches as desired. All of these things ought to be possible for you to achieve without having an impact on your regular life. Many consumers are unaware of how their data is gathered, utilized, and distributed online. The General Data Protection Regulation (GDPR) was strengthened in the European Union in 2018 to better secure our personal data. At the same time, significant campaigns are carried out annually to increase knowledge and awareness of cyber security. Data Protection Day and Cyber Security Awareness Month are two of these yearly occasions. Every year on January 28, there is an international celebration known as Data Protection Day. The day is meant to promote privacy and increase consumer, business, and individual awareness. Everyone will learn how to properly safeguard their personal information online in this way. The European Union conducts its yearly campaign known as Cyber Security Awareness Month (ECSM) every October. The campaign disseminates current knowledge about online security to organizations and EU residents.

2. METHODS

There are various measures to apply Cyber Security for protecting the Data

2.1. Conduct cyber security training and awareness

CyberSecurity Awareness (CSA) is a continuous process, and it is most effective when performed iteratively and focused on continuous improvement. It must comprehend factors like the evolving cyber threat landscape, advancements in technology, and shifts in an organization's missions and priorities to stay relevant to the target audience and optimized for the organization. But this is possible only if CSA programs are reviewed and evaluated for their effectiveness. Review and evaluation aim at evaluating the effectiveness of the undertaken iteration according to a set of pre-defined metrics, demonstrating in this way the achieved return on investment (ROI). [2] It is essential for reducing the dangers that could result in data breaches and other cybersecurity issues. There will be a greater awareness among workers of information security best practices, apps, and tools like social media, email, and websites that are frequently used at work.

2.2. Perform risk assessments

Organizations should do a comprehensive risk assessment to identify all important assets and rank them according to the impact a compromised asset will have. This will assist businesses in choosing how to allocate their resources to safeguarding each priceless asset.

2.3. Ensure vulnerability management and software patch management/updates

Hardware security advances serve to improve secure implementation of digital systems. Realizing such improvements depends on several non-technical factors, and will have to acknowledge cost-benefit perspectives across the cybersecurity ecosystem. There is little at present to indicate who the ultimate decision-makers are regarding adoption of secure hardware, given the lack of studies that reveal the decision process that governs adoption of new hardware; there are examples of existing research, which indicate factors of interest around the technical features of new hardware, for instance, for new Internet-of-Things devices. In comparison, there is a dearth of material on any particular decision-maker involved in secure hardware choices. This is exemplified by papers, which identify criteria for selecting hardware. Of interest is whether altogether different criteria are also involved in deciding whether to take on newly-available hardware. Secure hardware here includes concepts and technologies that fall under physical, structural and behavioural domains of hardware abstraction layers. [3]

2.4. Use the principle of least privilege

According to the principle of least privilege, both software and employees should only be given the permissions essential for them to carry out their responsibilities. This lessens the impact of a successful security breach because user accounts or software with lesser rights cannot affect priceless assets that need authorization at a higher level. Additionally, all high-level user accounts with unfettered rights must employ two-factor authentication.

2.5. Enforce secure password storage and policies

Businesses should require all employees to use secure passwords that follow industry-recommended best practices. Additionally, they should be required to be changed on a regular basis to assist against password breach. Furthermore, using salts and powerful hashing algorithms is one of the industry best practices for password storage.

2.6. Implement a robust business continuity and incidence response (BC-IR) plan

An organization will be better able to respond to cyber-attacks and security breaches while ensuring that crucial business systems stay operational if it has strong strategies and procedures in place.

2.7. Perform periodic security reviews

Periodic security inspections of all software and networks aid in spotting security risks early on and in a secure setting. Application and network penetration testing, source code reviews, architecture design reviews, red team evaluations, etc. are all examples of security reviews. Organizations should prioritize and mitigate security vulnerabilities as soon as they are identified.

2.8. Backup data

Regularly backing up all data will increase redundancy and ensure that no sensitive data is lost or compromised in the event of a security breach. The availability and integrity of data are compromised by attacks like ransomware and injections. In these situations, backups can assist protect.

2.9. Use encryption for data at rest and in transit:

Strong encryption algorithms should be used to store and transmit all sensitive data. Data confidentiality is ensured through encryption. Policies for efficient key management and rotation should also be implemented. Every web application and piece of software should use SSL/TLS.

2.10. Design software and networks with security in mind:

Always consider security whether developing applications, writing software, or designing networks. Remember that restructuring software and adding security features after the fact is much more expensive than including security right away. Applications with security features help to lessen dangers and make sure that software and networks fail safely.

2.11. Implement strong input validation and industry standards in secure coding:

The first line of security against different kinds of injection attacks is frequently strong input validation. Strong input validation helps filter out harmful input payloads that the application would process because software and apps are meant to receive user input, which makes them vulnerable to assaults. Additionally, when designing software, secure coding standards should be followed as they assist prevent the majority of the common flaws listed in CVE.

2.12. *Use virtualization:*

Not everyone needs to go this route, but if you do, be prepared to be inundated with spyware and viruses if you visit dubious websites. While avoiding risky websites is the best approach to prevent browser-derived incursions, virtualization enables you to run your browser in a safer environment that bypasses your operating system, such as Parallels or VMware Fusion. [5]

2.13. *Endpoint security:*

It implemented on endpoint devices, including as servers and worker workstations, which can fend off dangers like malware, illegal access, and the exploitation of operating system and browser vulnerabilities.

2.14. *Threat intelligence*

It integrates various feeds with information on threat actors and attack signatures, adding more context to security incidents. Security teams can detect assaults, comprehend them, and develop the best defence with the aid of threat intelligence data.

Once hackers have gained access to a system, mitigation and recovery can become time-consuming, expensive projects. So prevention becomes a crucial component of a cybersecurity programme. The following actions are advised: (a) implementing technical solutions for the encryption and interoperability of data; (b) strengthening the public key infrastructure (PKI) for identification; (c) conducting regular cyber risk assessments of the ID authority and its partners; (d) conducting regular audits of the ID authority's infrastructure and processes by external vendors; and (e) conducting regular penetration tests by certified ethical hackers and by the national CERT to identify potential threats.

A vital component of a cybersecurity programme is to quickly recover and return to normal operational levels in the event of a compromise. To do this, it is advised that you (a) create a business continuity plan that takes the ID ecosystem's business operations into account, (b) test and exercise that plan, (c) create a disaster recovery plan that considers the ID system's infrastructure operations, including redundancy, and (d) build related capacity [6].

The conceptual goal of using the three stages of threat prevention, detection, and reaction is to achieve a state of computer "security." These procedures are based on numerous system elements and policies, such as the following:

- System files and data can be protected using user account access controls and cryptography, respectively.
- From the perspective of network security, firewalls are by far the most prevalent prevention systems since they can (if configured correctly) guard access to internal network services and prevent specific types of assaults through packet filtering. Hardware- and software-based firewalls are also possible.
- Products from intrusion detection systems (IDS) are made to help with post-attack forensics by detecting network attacks as they are happening and by providing audit trails and logs for specific systems.
- The term "response" must be defined in terms of the system's evaluated security needs and might refer to anything from a straightforward safeguards upgrade to notifying the appropriate authorities, mounting counterattacks, and other actions. In some rare circumstances, it is preferred to completely destroy the compromised system because it is possible that not all of the resources have been compromised. [4]

3. MEASURES TO AVOID CYBER ATTACKS:

Although preventing cybercrime and guaranteeing total internet security may not be achievable, organisations can lessen their exposure to it by establishing a successful cybersecurity plan that uses a defense-in-depth strategy to secure systems, networks, and data.

- Be cautious while sharing personal information online. Alter your privacy settings and avoid using location services.
- Retain operating systems and software up to date.
- Use capital and lowercase letters, numbers, and special characters to create secure passwords. Utilize a password manager and two verification methods. Be wary of any activity that demands immediate action from you, makes an offer that seems too good to be true, or requests personal information. Before you click, consider. If unsure, don't click.
- Use a secure Internet connection and Wi-Fi network to protect your home and/or business, and update your passwords frequently.
- Don't divulge passwords or PINs. When possible, employ biometric scanning equipment (e.g. fingerprint scanner or facial recognition).
- Regularly check your credit reports and account statements.
- Exercise caution when disclosing private financial information such as your credit card number, Social Security number, or bank account number. Share personal information only on secure websites. Useless websites should not be used. Utilize a Virtual Private Network (VPN) to establish a connection that is more secure.
- Use firewalls, anti-virus software, and anti-malware programmes to block threats.
- Avoid clicking on links in texts or emails you get from strangers. False connections to websites can be made by con artists.
- Keep in mind that the government won't approach you about owing money by calling, texting, or using social media.
- Be aware that con artists may phone offering work-from-home opportunities, debt consolidation offers, and payback plans for student loans in an effort to capitalise on people's anxieties about their finances.[7]

4. PREVENT SECURITY BREACHES:

A security breach that exposes client data can result in financial damage for businesses and organisations. However, it may also result in a decline in client loyalty, confidence, and brand reputation. All businesses should be open and honest about how they gather, use, and share the data of end consumers. In order to protect data, they also need to have in place the security technology, security policies, risk management, and cyber security that are essential. In order to prevent cyberattacks, the company and its employees should establish clear policies and procedures, plan ahead for handling cybersecurity incidents, give an overview of the systems and data protection in place, install two-factor authentication (2FA) keys or use 2FA apps, enable 2FA whenever possible for all online accounts, and verbally confirm the legitimacy of money transfer requests by speaking with the financial manager.

To prevent security breaches, they may additionally examine each email request for a transfer of funds to see if it differs from the norm in addition to all these other precautions. Employees should receive ongoing training on cyber security protocols. Establishing a security culture requires that management and staff members have a similar vocabulary and understanding of the company's mission and goals. [12]

Building a security culture with the staff is essential; it cannot be forced upon them. A variety of technical, administrative, and other professionals must be included on the team that will administer the programme. They must have a thorough awareness of the company, its objectives, and the dangers it faces. This holds true for both minor threats and deliberate attacks. Cybercriminals cannot enter your company if you only rely on anti-virus software. However, training staff members to make wise cyber-defensive decisions can unquestionably lower the likelihood of cyber dangers! Moreover, training staff members in cyber security awareness and defence doesn't need to be done by an expert. Modern advanced technology-based solutions can assist and direct staff members in identifying and countering cyber threats before they compromise networks and systems.

Here, we focus on the decision-making processes and incentives for investment in secure hardware by decision-makers. This includes direct investment needs and indirect costs such as business disruption and adaptations to business processes. This will serve to add detail to the concept of success and failure for security technology investments, and inform what are perceived as successful decisions and the reasons as to why. [8]

5. IMPACTS OF CYBER SECURITY:

Businesses and individuals can safeguard themselves from the complete spectrum of cyber security dangers listed here as well as the many others that exist by putting security measures in place. Companies no longer have to worry about unwanted individuals accessing their network or data thanks to cyber security. They benefit from increased user and employee safety. Security speeds up recovery time even in the few instances when it cannot stop an attack or breach. Additionally, businesses frequently discover that users and programmers have greater faith in goods that are protected by reliable cyber security measures.

- ***It Can Protect Your Business*** The major benefit is that your company can get complete digital protection from the best IT security cyber security solutions. This will protect your staff from potential hazards while enabling them to use the internet whenever they need to**.**
- ***Protects Personal Info:*** Personal information is one of the most precious commodities in the digital age. A virus is highly capable of selling or even utilising personal information about your clients or employees to steal their money if it can get its hands on it.
- ***Allows Employees to Work Safely*** You and your staff are continuously at risk from a potential cyber-attack if your company doesn't have the best cyber security solutions. If your computer system, or even a single computer, gets infected, it can seriously reduce productivity and perhaps compel you to buy new ones.
- ***Protects Productivity:*** Viruses can make using personal computers nearly impossible by slowing them down to a crawl. This can result in a great deal of lost time for your staff and frequently causes the entire operation to halt.
- ***Stop Your Website from Going Down:*** Most likely, as a company, you host your own website. There is a very real danger that your website may have to go offline if your machine gets infected. This implies that in addition to losing money from declined transactions, you will also lose the trust of your customers and your system may be permanently damaged by some malware.
- ***Denies Spyware:*** Spyware is a type of online infection that is made to monitor your computer's activities and provide that information back to the online criminal. Excellent cyber security protection, can stop this spyware from working and guarantee that your employees' actions are kept private and secret at work.
- ***Prevents Adware:*** Adware is a popular type of computer infection that inundates your computer with advertising. All of these advertisements, though, can seriously hinder productivity and frequently let other infections into your computer when they are unintentionally clicked.
- ***A Consolidated Solution:*** The best security options for a company will provide a complete defense against a wide range of threats. A firewall, anti-virus, anti-spam, wireless security, and online content filtration are the ideal components of your security system**.**

- ***Inspire Confidence in Your Customers:*** Your consumers and clients will be more likely to have faith in your company if you can demonstrate that it is adequately safeguarded against all types of cyber threats. When acquiring your goods or utilizing your services, they will feel more assured.

Today's cyber security industry is primarily focused on protecting devices and systems from attackers. While the bits and bytes behind these efforts can be hard to visualize, it's much easier to consider the effects. Without cyber security professionals working tirelessly, many websites would be nearly impossible to enjoy due to ever-present denial-of-service attack attempts. Imagine not having access to Simplilearn's community of experts and certified professionals — no more tips, tricks, and advice to help you achieve your professional goals. [9]

A breach or other security catastrophe can be expensive, and it might take some time to fix and resume regular business operations. Employees who are familiar with cybersecurity concepts and are aware of their responsibilities. Fundamentally speaking, there is no indication that our civilization will become less dependent on technology. Identity theft-related data dumps are now openly announced on social media sites. Cloud storage services like Dropbox or Google Drive are now used to store private data including social security numbers, credit card numbers, and bank account information.

The significance role of cyber security is to protect networks, computers, programs from unauthorized access and loss. Most of the users are not aware of the risks and share their information unknowingly and their lack of knowledge makes them vulnerable to cyber-attacks. So cyber security is the main concern in today’s world of computing [10].

6. THREATS TO AN ORGANIZATION:

Any organisation could suffer a variety of grave repercussions from a data breach. It can ruin a company's reputation by alienating customers and business partners. A company's competitive advantage may be lost if crucial data, such as source files or intellectual property, is lost. Further, a data breach can reduce corporate profits because it violates data protection laws. An organisation that experiences a data breach is thought to lose $3.6 million on average. It's crucial that businesses create and put into practise a comprehensive cybersecurity strategy in light of the media attention that high-profile data breaches have received. [11] Website crashes are prevented by cyber security: If you own a small business, you presumably host your own website. There is a considerable chance that your website will be forced to go down if your system becomes infected. This implies that in addition to suffering losses from omitted transactions, you also face the danger of alienating your customers and having your systems seriously damaged by malware. [12]

7. PREVENTIVE TECHNIQUES WITHIN THE ORGANIZATION

Organizations should have a cyber threat intelligence (CTI) capacity that can enable them quickly identify, detect, and respond to attacks if they want to address cyber risks successfully. Cyber threat intelligence is the proactive collection, analysis, and dissemination of intelligence both internally and externally with the goal of enhancing security. It involves the use of technology, processes, and people. The CTI strategy places a strong emphasis on situational awareness and tactical or strategic solutions that might aid in lowering the danger or chance of harm to your organisation. A CTI strategy focuses on a company's capacity to quickly combine internal and external intelligence to create a "situational awareness" that will be integrated into the company's overall security posture. For information assets to remain confidential, intact, and accessible, CTI is essential.

Human interaction is important, in addition to a variety of technology-related goods and services that can assist a company in enhancing its CTI capabilities. Participating in industry associations can give your company access to information on security techniques and trends used by competitors, as well as a forum for exchanging personal experiences with your peers to help build consensus and raise awareness of cybersecurity challenges.

external perception Learn about the locations and characteristics of cyberattacks that affect your industry. Look for fresh information sources. Share that information with others in your sector, your business partners, and in particular any other organisations that you exchange data with on a regular basis.

Keeping track of data access activities can help you strengthen your overall security posture since it leaves a trail that you can follow and investigate. It's crucial to continuously track and examine your data trails. Do you actually understand what's going on in your company? Do you understand what happens to your data as it passes between mobile and cloud applications and as it is handled by your partners? Many businesses maintain activity records solely for regulatory compliance. However, logs might provide strong hints for identifying less visible hazards to your company. Logs can assist you in finding trends or occurrences that point to a less obvious breach or a potential data gap that has to be closed. Do more than simply look over your log data and related data. For insight, use it. By doing this, you can quickly identify a threat. In order to establish an enhanced detecting capability, you might need additional tools. To efficiently manage huge volumes of security data and look for suspicious patterns—to identify that threatening needle in the haystack-more advanced enterprises are increasingly implementing sophisticated security-analytics systems.

The sophistication of the exploit techniques and methodologies used by cyber adversaries, actors, and criminal organizations continues to rise, and they will keep developing their strategies. Some of these techniques get through both more advanced protection systems and conventional cyber defenses. And using sophisticated threat methodologies, cybercriminals are concentrating in particular on an attack vector that preys on company users, employees, and partners. These methods are frequently created with espionage or financial gain in mind, or they are concentrated on other objectives that might have a significant impact on business. Organizations must put their efforts into developing a multilayered strategy to defend against cyberattacks in light of the threats' increasing complexity and impact

Organizations can provide a "last line of defense" against many of these sophisticated attacks by relying on end-user attentiveness, training, and awareness. More should go into security awareness than just following regulations. Your goal should be to alter the organisational culture around security and employee behaviour. Creating awareness involves creating a culture. The more individuals considering cybersecurity, the more alert your firm will be. To do this, keep enticing employees who are not part of the IT team to consider cybersecurity, to consider not only the technical difficulties but also the business and process challenges. Each group of participants must be aware of what is expected of them by the organisation, what is at risk, and what they must be doing.

Furthermore, it's critical to inform your company's employees that cyber hazards go beyond IT issues. Internal and external system users are ultimately responsible for overall security since they are a people problem and a business problem. That argument might be difficult to convey, particularly if staff members find the increased security measures to be burdensome or inconvenient. In order to ensure that users understand security concerns and regulations, organisation leaders should create training and awareness initiatives. Additionally, they should make sure that each area of leadership-whether it is IT leadership or another area of business leadership—is aware of the cybersecurity initiatives and messaging for which they are accountable. And when it comes to security awareness, leadership must create "tone at the top"

Additionally, workers need to be made aware of particular hazards and their possible repercussions. Workers should be on the lookout for "spear-phishing" tactics, for instance, where a hacker uses personal or customised information to target a specific user (for instance, through an email message with phoney corporate links) before ultimately infiltrating or infecting the broader organisation. For instance, a phoney "internal revenue report" email attachment that was sent to salespeople may contain malware that could harm the network of the company. Organizations can engage employees and partners by approaching awareness in a more dynamic, continuing way, making dangers seem more immediate, and emphasising the importance of each employee's involvement in securing the company.

CONCLUSION

Fix detected flaws The "known vulnerability" issue can be resolved with straightforward due diligence. This due diligence will need effort and time. Additionally, it should be carried out using a risk-based methodology, with IT departments collaborating with other internal decision-makers to help establish priorities in accordance with your business, your restrictions, and your current controls. Work to comprehend what is feasible given the personnel and technological expertise at your disposal.

Designing in security Security risks might also be present when developing software. Security protocols are frequently seen as a barrier or as something that can impede the timely creation of new technologies. However, development activities offer several chances to disregard security requirements or introduce new security flaws. The development process should incorporate security measures and a security attitude, according to organisations. And addressing the software side of security is insufficient. Additionally, you need to look for physical security flaws and gaps that could let an unauthorised person, a resentful employee, or an unknowing employee take or leak sensitive data. It can be more difficult to address possible gaps in physical security and access rights. Establishing roles, responsibilities, and protocols for data access as well as physical access to locations within your company can help it become more secure.

Using novel polymorphic security warnings: According to Anderson et al. (2015), most people ignore security warnings on the internet due to habituation. In the field of psychology, habituation refers to a decreased response to repeated exposure to the same stimulus over time (Rankin et al., 2009). That is, we do not pay attention to objects that we repeatedly see. West (2008) also argued that most warning messages are similar to other message dialogs. Accordingly, computer system users often ignore them, as our brain is not likely to show novelty and attentional allocation response to such security warnings (Moustafa et al., 2009). [13]

Cybersecurity usually faces some difficulties, but there are always solutions to strengthen security in such circumstances. The main problem with cyber security is that it is constantly evolving, giving thieves a never-ending supply of new possibilities to try to take advantage of. This is made much more difficult by the ongoing innovation of cyberattack techniques by cybercriminals.

As a result, developers of cyber security software and industry professionals consistently come up with fresh fixes to plug potential holes, only for hackers to keep coming up with new ways to launch an assault. As a result, cyber security is always changing. The constantly changing nature of cyber security makes it extremely difficult and expensive for enterprises to keep current. It necessitates ongoing updates as well as persistent attention to the security sector.

Future work will engage with stakeholders in organizations adopting hardware, building case studies in a vertical manner. This would involve the decision-makers responsible for determining whether to adopt new hardware in systems and products, as well as those involved in engineering and implementation, and their assessments of how to integrate new solutions into existing systems. This would build a picture that relates the value proposition for the business to the efforts to align new hardware with existing technology to realise that value. [14].

CONSENT FOR PUBLICATION

Not applicable.

FUNDING

This study was supported by The Scientific Research Projects Unit of Bursa Uludag University [KUAP(T)–2020/9].

CONFLICT OF INTEREST

The authors declare no conflict of interest, financial or otherwise.

ACKNOWLEDGEMENTS

Declared None

REFERENCES

[1] Cyber Security Essay for Students and Children Available at: https://www.toppr.com/guides/essays/cyber-security-essay

[2] Chaudhary, S.; Gkioulos, V.; Katsikas, S. Developing Metrics to Assess the Effectiveness of Cybersecurity Awareness Program. *Journal of Cybersecurity* **2022**, *8* (1). https://doi.org/10.1093/cybsec/tyac006.

[3] Tomlinson, A.; Parkin, S.; Shaikh, S. A. Drivers and Barriers for Secure Hardware Adoption across Ecosystem Stakeholders. *Journal of Cybersecurity* **2022**, *8* (1). https://doi.org/10.1093/cybsec/tyac009.

[4] What Is Cyber Security and How Does It Work? | Synopsys https://www.synopsys.com/glossary/what-is-cyber-security.html (accessed 2020 -10 -31).

[5] Freedman, M. How to Secure Your Computer From Hackers https://www.businessnewsdaily.com/11213-secure-computer-from-hackers.html.

[6] Implementing a cybersecurity program | Identification for Development https://id4d.worldbank.org/guide/implementing-cybersecurity-program (accessed 2022 -04 -30).

[7] Ready.gov. Cybersecurity | Ready.gov https://www.ready.gov/cybersecurity.

[8] Tomlinson, A.; Parkin, S.; Shaikh, S. A. Drivers and Barriers for Secure Hardware Adoption across Ecosystem Stakeholders. *Journal of Cybersecurity* **2022**, *8* (1). https://doi.org/10.1093/cybsec/tyac009.

[9] Kelley, K. What is Cybersecurity & Importance of Cyber Security | Simplilearn https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security#:~:text=Cybersecurity%20is%20crucial%20because%20it (accessed 2022 -09 -28).

[10] Ghundare, S.; Patil, M.; Lad, R. *Importance of Cyber Security*; 2020.

[11] **Cyber Security**; Available at: https://cio-wiki.org/wiki/Cyber_Security#The_Importance_of_Cybersecurity.5B3.5D

[12] Essay On Cyber Security | Importance, Risks & Challenges https://mystudentsessays.com/essay-on-cyber-security/ (accessed 2022 -04 -25).

[13] Moustafa, A. A.; Bello, A.; Maurushat, A. The Role of User Behaviour in Improving Cyber Security Management. **2021**. https://doi.org/https://www.frontiersin.org/articles/10.3389/fpsyg.2021.561011/full

[14] Tomlinson, A.; Parkin, S.; Shaikh, S. A. Drivers and Barriers for Secure Hardware Adoption across Ecosystem Stakeholders. *Journal of Cybersecurity* **2022**, *8* (1). https://doi.org/10.1093/cybsec/tyac009.