www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 12 Issue 11 November 2023, Page No. 25948-25953
ISSN: 2319-7242 DOI: 10.18535/ijecs/v12i11.4777

Cybersecurity Best Practices: Strategies for Protecting Organizations from Cyber Threats

Ankita Banerjee[1], Ankita Paul[2], Anirban Bhar[3], Dhriti Chakraborty[4]
[1,2] B. Tech student, Department of Information Technology, Narula Institute of Technology, Kolkata, India.
[3,4] Assistant Professor, Department of Information Technology, Narula Institute of Technology, Kolkata, India.

Abstract
The academic and practitioner literature on the topic of information security is extensive. The majority of the study is concentrated on finding technology remedies to security threats, however other methods like deception, reaction, detection, and deterrent are also being considered. This article presents the results of a qualitative study that was carried out in Korea with the aim of discovering the security measures that companies employ to safeguard their information systems. Based on the findings, it is clear that there is a widespread ignorance of business security issues and a strong emphasis on taking precautions to guarantee the availability of services and technologies. There were additional strategies, but they were all preventative. With an emphasis on integrating, balancing, and optimizing systems, the paper lays forth a research agenda for implementing various techniques across a company. This study examined a wide range of issues, including data protection and potential meeting places for security strategy discussions, like military archives. In all, nine different security measures have been recognized. The utilization of various security techniques in enterprises is investigated through a qualitative focus group approach. The goal of the focus groups was to get the security managers from eight different companies to talk about the security measures their companies take. The results show that many companies take precautions to ensure that their technological services are always available. In order to back up the prevention strategy operationally, some of the other methods that were identified were utilized.

Keywords: Cyber Security, Cyber Threats, Domain, Framework.

1. Introduction

Companies are starting to realize the importance of information and related technologies across the board, but especially in fostering innovation and creating a competitive edge. The security of corporate information and technology services is a major concern in today's information world. Leaks of sensitive data and long periods of downtime for email and internet access are two examples of the many threats that can affect business continuity. Establishing a thorough framework for the development, institutionalization, assessment, and enhancement of an information security program is essential for any organization looking to adopt an information security strategy and manage these security concerns. In instance, the information security strategy's content ought to be able to be traced back to these higher-level sources in order to demonstrate its support for the organization's overall strategic intentions. [1]. Security incidents are on the rise, despite the fact that most firms implement "baseline" security procedures. Researchers found that more than 60% of companies implement technical measures to protect sensitive information. These methods include firewalls, antivirus software, anti-spyware software, VPNs, vulnerability/patch management, data

encryption in transit, and intrusion detection systems. Organizations have been consistently targeted in these attacks, according to these reports. An growth in both internal and external threats, according to these same research, makes security risk higher. Consequently, security is getting harder to handle. To thrive in this setting, businesses need to make the most of their limited resources while strategically directing their security efforts. But it's possible that a single system won't cut it [1]. Businesses should use several information security strategies, according to the argument, to keep security rules in place and make sure security measures work. A large body of research has concentrated on the nuts and bolts of information security, such as security controls and how to put them in place to 'avoid' security breaches in companies. A number of other security tactics, such as detection, deterrence, and deception, have been proposed in the literature alongside prevention. There is a lack of data on the specific security measures taken by different types of companies in response to different types of security threats [2]. The majority of security administrators paid little attention to threats to company data. Instead of following a methodical and well-planned approach to risk management, plans were often implemented on the fly [3, 4].

2. Literature Review

The most accurate description is "figuring out what to use, how to use it, and how to apply it" in a military context. Strategy is defined by Beckman and Rosenfield (2008) as "deciding where your business wants to go and finding out how to get there." An information security plan can be constructed using these explanations. According to these viewpoints, Information security strategy, according to Perk et al., is the "art of deciding how to best utilize what appropriate defensive information security technologies and measures, and of deploying and applying them in a coordinated way to defense organization's information infrastructure(s) against internal and external threats by offering confidentiality, integrity, and availability at the expense of least efforts and costs while remaining effective." Methods such as deception, perimeter defense, compartmentalization, layering, surveillance, detection reaction, and prevention have been found through research [1–5]. After reviewing the relevant literature, two crucial aspects of strategy were apparent: time and geography. It is possible to execute plans either in advance of or in response to an attack. Looking at the 'battlefield' setting through a spatial perspective is crucial. One way to stop an untrusted computer system from getting into a trusted region is to create different zones for trustworthy and untrusted computer systems on the battlefield. Lastly, from a decision-making perspective, strategy is affected by the selection of certain attack and reaction tactics. The literature-based method is defined and described in the sections that follow [1, 2, 6, 7].

3. Cybersecurity, knowledge and strategy

A potential precursor Many prominent schools of thought in organizational theory and strategic management over the past 30 years have relied on interpretations of knowledge as a construct. Examples include knowledge management, the company's knowledge-based vision, and dynamic capabilities. Some have questioned the effectiveness of these endeavors due to factors such as a lack of clarity in the interpretation of knowledge, differing opinions on the practicality of the goals, a lack of unity in the themes that were originally intended to advance society, and, finally, the fact that they failed to avoid Occam's razor. This historical use of "knowledge" as an explanatory or prescriptive notion reveals regularities worth noting when used to an epistemic approach to organizational cybersecurity strategy. An intellectual undertaking is the search for the "effective," or at least the lasting epistemic foundation, of ideas in the field of organizational theory. Conversely, the vast body of literature on the topic offers a pattern of critical features that contextualize specific conceptualizations. There is a close relationship between an individual's epistemological stance and their views on the nature, function, and reachability of truth as well as their views on the embodiment and form of knowledge (the known). Regarding the relational positioning of

uncertainty, we also think it's contextually relevant [5,8].

4. Best practices for cyber security

Computers and the Internet are ubiquitous today. These systems store, modify, and share personal and business data daily. Cyber security protects data by preventing, detecting, and responding to vandalism, theft, and corruption. Organizations must address cyber security for many reasons. People and employees who give an organization personal information want it to be respected and protected. Organizational data must be protected. Your partners and service providers will seek assurance that electronic transactions will not compromise their data and systems. Finally, regulations demand protecting numerous forms of data. HIPAA, FERPA, and PCI DSS apply if your company provides employee health benefits, operates a school, or accepts credit card payments. No firm can create a perfect cyber security plan. Instead, firms should establish and review cyber security measures that secure sensitive data and make their systems and networks hard to hack. This section covers basic cyber security best practices for your company.

4.1. Implement cyber security policies and train staff

Make sure everyone on staff knows how to use the company's computers and other IT devices correctly. The term "sensitive data" and the many forms it takes should be defined. Make it crystal clear what information needs to be protected and how it will be protected. Make and follow rules that spell out how to deal with and safeguard confidential information. Make cyber safety a priority by training all employees and volunteers in fundamental security procedures. Raise company-wide security consciousness and educate employees.

4.2. Protect information, computers and networks from cyber-attacks

Prevent cyber-attacks on data, systems, and networksTo safeguard computers and other electronic devices against spyware, viruses, and other harmful programs, it is recommended to install anti-malware and anti-virus software. Another line of defense against these dangers is to always use the most recent versions of operating systems, web browsers, and security software. Having antivirus and anti-malware software set to automatically update and run in "real-time" mode allows for continuous threat monitoring and mitigation. Along with real-time security, every computer should be scanned weekly for viruses and spyware.

4.3. Updating operating systems and apps

Operating system and application software vendors are always releasing updated versions of their products and releasing patches and remedies for bugs as soon as security holes are found. When new versions or updates become available for computers and other technological equipment, it is crucial to keep them updated. Companies like Apple and Microsoft typically plan to deliver updates on a regular basis, but they might release a patch to fix a critical vulnerability whenever it arises. The majority of OSes include the option to either notify the user or perform automatic updates when new versions become available. It is recommended to periodically upgrade to new versions, patches, and fixes for all operating systems and application software.

4.4. Secure your Internet with a firewall

All day, every day, most businesses leave their computers vulnerable to outside attacks because they use a "always on" Internet connection. In order to prevent these dangers, firewalls are essential for computers that are linked to the Internet. Firewalls can be bought from firewall manufacturers, included in routers or wireless access points, or offered as a service by your Internet service provider. Regardless of the kind, it is important to constantly apply product updates and change administrative passwords both when launched and

on a regular basis thereafter. It is recommended to enable the built-in software firewall capability on most computer operating systems. Employees that do remote work should have a firewall in place and be subject to your company's cyber security policies and procedures.

4.5. Plan mobile device action

If a mobile device—such as a smartphone, tablet, laptop, memory stick, or hard drive—contains sensitive information or has access to your internal network, data security becomes a major problem. In order to prevent information theft while the device is working, particularly over a public network, limit their use wherever possible and make users encrypt stored data, enable password protection, and install security apps. Make sure that employees know what to do in the event that their mobile devices are stolen or misplaced.

4.6. Make backups of vital corporate data

Back up all of your machines' data on a regular basis. Files pertaining to human resources, finances (including accounts receivable and payable), databases, spreadsheets, and word processors are all considered critical data. Perform a full backup every night and automated backups during the day if at all feasible. Back up your systems at least once a week. Keep a copy off-site or in the cloud for safekeeping. All off-site data storage locations must encrypt data including sensitive personal, financial, or medical information. Set up and test a procedure to restore data to the system regardless of how often or where copies are kept.

4.7. Limit physical computer access and create staff user accounts

Ensure that no unauthorized individuals are able to access or utilize company computers. Using a privacy screen or moving the monitor is recommended in cases when sensitive data is shown on computer screens and could be accidentally seen. Put in a password to lock the computer and use screen savers if you can. Make sure to physically protect your laptop whenever you're not using it to prevent theft or misplacing it. Each employee must have their own user account and must utilize strong passwords. Only essential staff should have administrative-level access.

4.8. Secure wireless networks

If your company uses a Wi-Fi network, you should encrypt all data transfers using the latest industry standards. Put a strong password on the router's administrator account. Separate the guest Wi-Fi network from your company's main Wi-Fi network if your company offers that service.

4.9. Limited data and information access; program installation

When feasible, restrict the conditions under which a single employee can access all company databases. Rather, you should restrict staff access to certain systems according to the needs of their individual job functions. Nobody on staff should be able to install programs without management's explicit consent. You might want to think about implementing content monitoring and filtering systems on machines that have Internet connection.

4.10. Passwords and authentication

Make sure that every employee uses a different password and changes them at least once every three months. A combination of uppercase and lowercase letters, numbers, and special characters, spanning at least 6 to 8 digits, is ideal. Think about adding a layer of security that takes more than just a password to access your account. If you do business with companies that deal with sensitive information, particularly financial institutions, you should inquire as to whether or not they provide multi-factor authentication for

your account.

4.11. Don’t forget embedded systems and other often missed data sources

The HVAC, lighting, security, and telephone systems of many businesses are monitored and controlled by specialized computers. These computers are typically linked over the Internet and can run alone or with the help of remote staff. If at all feasible, use a separate Internet connection and keep these systems totally segregated from the rest of your company's PCs. To further protect sensitive information and stop the spread of infection, these devices should be electronically quarantined from other devices and PCs if full isolation is not feasible. Internal memory or hard disk drives are occasionally included in devices including fax machines, printers, scanners, and copiers. Before removing these devices from service, make sure all internal storage is properly wiped.

4.12. Payment Cards

Credit card processing companies have a responsibility to protect their customers' personal information. If you can help it, have a third-party institution handle credit card processing whenever possible. Retain only the information that is absolutely necessary and dispose of the rest securely if credit card processing is done internally. Physically separate the computers used to process payments from any other computers in the organization and strictly regulate employee access to these systems. It is important that computers used to process credit card payments are not allowed to access the Internet.

5. Conclusion

Using a methodical strategy for the literature review and a qualitative analysis of the selected articles, this study investigated cybersecurity concerns within the context of Industry. There were four main points covered in the analysis of the articles. First, we'll take a look at what cybersecurity is and how it's defined in the industry. Then, we'll identify the types of industries and industrial assets that are most vulnerable to cybersecurity threats. Third, we'll define system vulnerabilities, cyber threats, risks, and countermeasures for industry scenarios. Lastly, we'll find guidelines and more organized solutions to solve cybersecurity issues. Consequently, a reference framework was created outlining the key components of each sector. To give a quick chance of synthesis that can be utilized to direct future study and management operations, the framework compiles and summaries the most cited evidence for each area of inquiry. Although many solutions have been developed to address cybersecurity issues in industry, none of them consider the fact that cyberattacks can exploit all three layers of Cyber-Physical Systems (physical, network, and computation) simultaneously. The articles we looked at also take an information technology (IT) rather than a management (M) perspective on cybersecurity. Businesses could benefit from a management perspective when it comes to effectively implementing new organizational practices and change management initiatives. To address industry investigations and expand the present state of the art, future research can use this study as a basis.

References

1. Mosteanu, N. R., Artificial intelligence and cyber security– face to face with cyber attack–a maltese case of risk management approach. Ecoforum Journal, 2020. 9 (2).
2. Soni, V. D., Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. Available at SSRN 3624487, 2020.
3. Patil, P., Artificial intelligence in cybersecurity. International journal of research in computer applications and robotics, 2016. 4(5): p. 1-5.

4. Sagar, B., et al. Providing Cyber Security using Artificial Intelligence–A survey. in 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC). 2019. IEEE.
5. Sedjelmaci, H., et al., Cyber security based on artificial intelligence for cyber-physical systems. IEEE Network, 2020. 34 (3): p. 6-7.
6. Mohammed, I. A., ARTIFICIAL INTELLIGENCE FOR CYBERSECURITY: A SYSTEMATIC MAPPING OF LITERATURE. ARTIFICIAL INTELLIGENCE, 2020. 7(9).
7. Yampolskiy, R. V. and M. Spellchecker, Artificial intelligence safety and cybersecurity: A timeline of AI failures. arXiv preprint arXiv:1610.07997, 2016.
8. Morel, B. Artificial intelligence and the future of cybersecurity. in Proceedings of the 4th ACM workshop on Security and artificial intelligence. 2011.