IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 13, Issue 8, August 2024

DOI: 10.17148/IJARCCE.2024.13832

Robust Cybersecurity Measures: Strategies for Safeguarding Organizational Assets and Sensitive Information

Phani Durga Nanda Kishore Kommisetty[1], Valiki dileep[2]

Director of Information Technology[1]

Software Architect[2]

Abstract: Purpose: The purpose of this chapter is to introduce the reader to the theory and practice of cybersecurity, the main understanding of cybersecurity, the challenges faced globally, the security principles, and the security models for protecting the information security chain from various threats. In the second part of the chapter, we will introduce the critical aspects of the robust cybersecurity model, which was developed within the framework of the UPBAL project "Be Secure" and which gained further development in the F182 project on smart grid security.

Design/methodology/approach: The theoretical part of the chapter is based on the General Systems Theory, on which the main understanding of cybersecurity appears, while the current results are based on the experience achieved within the framework of the two mentioned projects, evaluated in the Piloting Reports, and theoretical strategies of other cyber defense-related theories. The theoretical principles are illustrated by several real-life practical examples from the field of ICT security.

Findings: As it is quite difficult to find any wider theories and practical documents that are oriented only to the needs of the development of the principles of a concrete area of cybersecurity, the concepts and strategic steps proposed could be of potential use to researchers and experts in this field, to discover the importance of developing a wider cybersecurity theory, find approaches within generalized methodology, as well as study and apply already developed criteria aspects and principles.

Keywords: Cybersecurity, Challenges, Security principles, Security models, Information security, Robust cybersecurity model, UPBAL project, Smart grid security, General Systems Theory, ICT security

I. INTRODUCTION

The quick acceleration of the implementation of digital technology globally to facilitate and improve business operations, in addition to abundant available sophisticated tools, has made the commercial solution of choice for many enterprises around the world. This ensures operational efficiency and effectiveness, but it has also rendered organizations vulnerable to attacks and intrusions from the outside world. These attacks and breaches demonstrate that enterprises are limiting their options by relying solely on technology to protect their assets and resources. Effectively addressing cybersecurity issues requires more than just acquiring and implementing the latest technology.

For a robust organization's cybersecurity posture to be effective, it must be dynamic and take into account people, politics, technology, and the nature of the business environment. It should use this knowledge to acquire and purposefully use a mix of critical capabilities to identify, stop, and mitigate the consequences of any data breach. Communication of the events to relevant authorities and stakeholders is also crucial. All businesses, regardless of their age, processes, industry, focus, size, product suite, resource level, or governing authority, should be aware of the risk of experiencing a data breach and the need to develop robust cybersecurity measures.The objective of this book is to provide organizational decision-makers, policymakers, and stakeholders with guidance on developing a secure cybersecurity posture. This will enable them to recognize and respond to new opportunistic threats associated with rapidly evolving technologies and threats. Cybersecurity should encompass technology, people, regulation, and process. By addressing regulatory, technology, and people issues holistically and bridging the gap between enhancing business operations and dealing with a changing threat landscape. This holistic approach also helps management maintain the necessary security posture that aligns with business objectives. The objective of this book is to provide organizational guidance by using a combination of contemporary academic thought, advice from US government policies and regulations, and global business capabilities and initiatives. These sources provide the best available approximations of cybersecurity and insights into this complex need.[9,1]

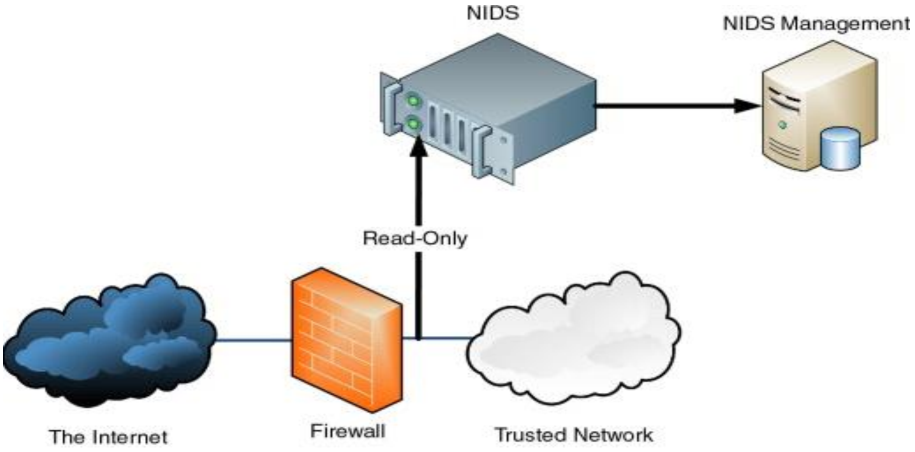

Fig 1: System Intrusion

1.1. Background and Importance of Cybersecurity in Organizations

Cyber threats pose a serious and ever-growing strategic risk to a range of organizations in the private and public sectors. They may include damage to brand or reputation, theft or corruption of sensitive information, direct financial losses, and theft of valuable intellectual property and data. Recognizing the increasing importance of cybersecurity as a core concern, organizations are investing in protective measures. Investments in cybersecurity are projected to reach $170 billion by 2020. The role of information leadership, security management, risk perception, and human behavior in cybersecurity have been identified in both academic theory and previous research. These protective measures include multiple layers of defense and monitoring which align with practices for ensuring the physical security of valuable organizational assets.The development of a comprehensive cybersecurity "law and economics" research and policy agenda that incorporates and focuses on the likely misalignment of incentives within the relevant organizations is a significant strategic challenge in the current environment. Our chapter aims to highlight some early-stage theoretical and conceptual bedrock on which those research and policy agendas can be built in the future. We hope that our contribution encourages further academic inquiry within computer and information science, risk and security management, and broader organization behavior disciplines on the industry's most pressing issues in cybersecurity.Cyber threats pose a serious and ever-growing strategic risk to a range of organizations in the private and public sectors. They may include damage to brand or reputation, theft or corruption of sensitive information, direct financial losses, and theft of valuable intellectual property and data. Recognizing the increasing importance of cybersecurity as a core concern, organizations are investing in protective measures. Investments in cybersecurity are projected to reach $170 billion by 2020. The role of information leadership, security management, risk perception, and human behavior in cybersecurity have been identified in both academic theory and previous research. These protective measures include multiple layers of defense and monitoring which align with practices for ensuring the physical security of valuable organizational assets.[15,18]

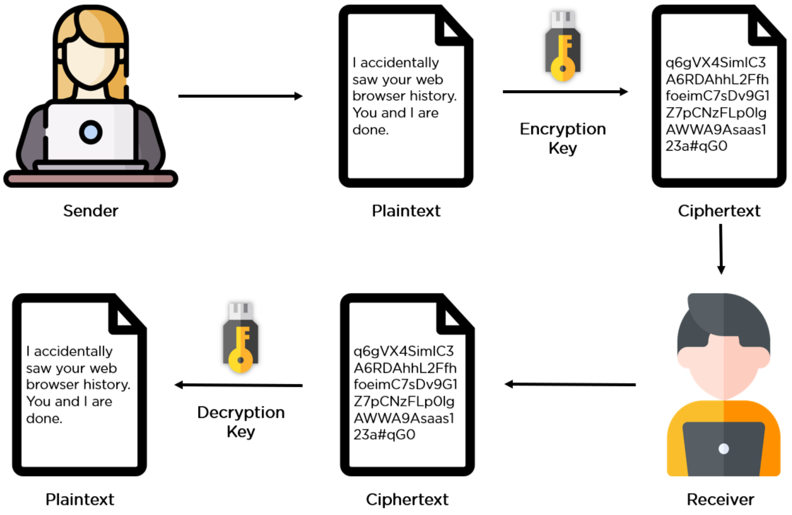
I accidentally saw your web browser history. You and I are done.
q6gVX4SimIC3 A6RDAhhL2Ffh foeimC7sDv9G1 Z7pCNzFLp0lg AWWA9Asaas1 23a#qG0
Encryption Key
Sender
Plaintext
Ciphertext
I accidentally saw your web browser history. You and I are done.
Decryption Key
q6gVX4SimIC3 A6RDAhhL2Ffh foeimC7sDv9G1 Z7pCNzFLp0lg AWWA9Asaas1 23a#qG0
Plaintext
Ciphertext
Receiver

Fig 2: Data Encryption Process

DOI: 10.17148/IJARCCE.2024.13832

II. COMMON CYBER THREATS AND VULNERABILITIES

However, cyber-attacks affect every individual and legal entity to some extent. Cybercriminals aim to damage or steal critical systems, power, electricity, water supplies, emergency services, communications, transportation, military intelligence data, financial reports, business plans, defense intelligence research data, and other important documents. In addition, often the biggest affairs depend more on knowledge capital than physical sources. Information is often one of a company's most important possessions. Large and small companies are constantly seeking and storing important information to achieve a high-quality, competitive edge.

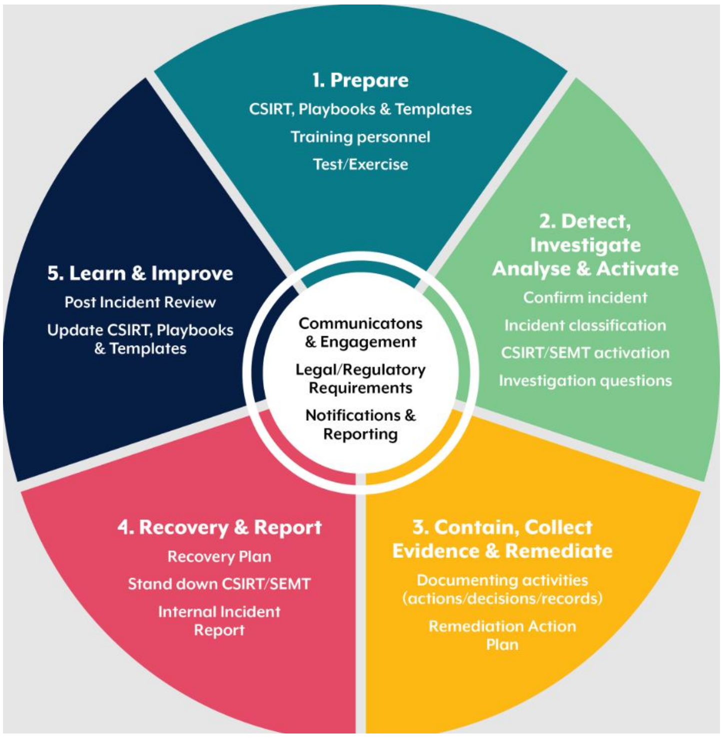
1. Prepare
CSIRT, Playbooks & Templates
Training personnel
Test/Exercise
2. Detect, Investigate Analyse & Activate
Confirm incident
Incident classification
CSIRT/SEMT activation
Investigation questions
3. Contain, Collect Evidence & Remediate
Documenting activities (actions/decisions/records)
Remediation Action Plan
4. Recovery & Report
Recovery Plan
Stand down CSIRT/SEMT
Internal Incident Report
5. Learn & Improve
Post Incident Review
Update CSIRT, Playbooks & Templates
Communicatons & Engagement
Legal/Regulatory Requirements
Notifications & Reporting

Fig 3: Cyber Security Incident Response Planning

2.1. Overview of Common Cyber Threats

The set of statistics on cybercrime can be overwhelming. For example, in a report presented by Accenture, a reduction of 19 percent in the total number of breaches in 2017 was reported. The remaining 81 percent was linked to several hacking tactics. But what are these tactics? How should we interpret the hard data about cyber threats and how can organizations deal with the very likely probability that their systems will be interrupted by cyber-attacks?Brute Force Attacks: A brute force attack is an attempt to discover a password by systematically trying every possible letter, number, and special character combination until the correct one is found. The criminals launch automated tools that brute force their way into the victim's databases and applications to acquire legitimate access for hacking incidents and other unauthorized activities. Many victims are unaware that nighttime rivalry between hackers and network administrators is not uncommon. Even though security is a round-the-clock task, security experts devote regular office hours to preventing intrusion attempts, but not all database attacks occur during business hours. This is the reason why some long-duration brute force attacks are so efficient: they take place during off-hours when potential victims are off-guard.[2,6]

2.2. Identification of Key Vulnerabilities

Several options are available for identifying an organization's key vulnerabilities. Professionals often focus their attention on infrastructure security but often neglect what is happening inside the physical building. A few key strategies for identifying vulnerabilities include (ISC), Defense In-Depth, Zero Trust, and the National Cybersecurity Center of Excellence (NCCoE). All of these strategies rely on a diligent workforce dedicated to finding vulnerabilities and securing discovered weaknesses. Once vulnerabilities are discovered, taking the next step and announcing them to the affected stakeholders can be a challenging and lengthy conversation. Identifying the most important vulnerabilities can quickly become an exercise in determining what is worth protecting and how much it is worth. With seemingly endless vulnerabilities, organizations can often feel paralyzed and unable to take action or implement any effective changes.

The federal government has attempted to make information sharing regarding cybersecurity incidents easier and faster with the establishment of Information Sharing and Analysis Centers (ISACs). The guidelines and standards developed by the ISACs are expected to change frequently in response to continually emerging threats and their ever-evolving tactics. Small businesses, however, are arguably left with the short end of the stick since they often cannot afford to employ a full-time cybersecurity professional.

III. STRATEGIES FOR ROBUST CYBERSECURITY MEASURES

A recurrent theme in "best practices" for corporate governance and risk management is the importance of an organization clearly understanding the nature of and risks to its most important assets. With the advent and rapid proliferation of information technology, many of these most important assets subsequently became "intangible" in nature. At the same time, the growth of data and information combined with the ease of access and relatively low cost of the Internet, have left organizations increasingly dependent on IT systems to store, manage, provide access to, and use information and data, both tangible and intangible. In the wake of cyber-attacks on very large corporations carrying high profiles in their respective industries, organizations are increasingly recognizing that the loss of intangible assets in cyber attacks can have severe effects on productivity and growth, corporate reputation, customer loyalty, stock price volatility, and compliance costs, to name but a few.

The increasing prevalence of technology in nearly every aspect of corporate and organizational existence has naturally been met by a growing concern over the security risks engendered by the same: the technological sophistication of cyber criminals seems to keep pace with the efforts of the organizations they target. In terms of national security strategies, these advances are enhanced by the existence of "the Dark Web," a corner of cyberspace that enables criminal networks to enjoy somewhat of a refuge from law enforcement.

Cyber-attacks not only affected confidential personal information but also led to society-wide disruptions when state actors use malware to add computers to botnets to cripple national infrastructure or implant itself for later mischief. Moreover, the lingering economic tremors after an attack, both from an organizational and macroeconomic viewpoint, have the potential to be severe. This chapter aims to consider ways in which organizations can enhance their economic resilience by implementing robust cybersecurity strategies.[5,7]

3.1. Risk Assessment and Management

Risk assessment is a critical and necessary first step for efficient and effective cybersecurity. In addition to determining the organization's aggregated information security risk, this initial process provides the foundation for pinpointing and auditing the right IT resource investments and could help determine the most cost-effective cybersecurity strategy. Risk assessment is a prerequisite for both the Information Security Plan and Security Incident Response Plan. They also help organizations recognize and establish accepted rules for key private and secret data. After those resources and data are categorized, they can even prioritize where the resources are required and allow the organization to have the greatest cybersecurity advantage.

Risk assessment manages and reduces the complexity of an information management program. They still allow the organization to concentrate mainly on priorities and to define reasonable budgets so that the most necessary tasks are handled. The scope of an access control request can be confined to the least amount needed to distribute information and fulfill the "reputation organization" requirement for the information. Preparing for a hazardous event results in less chance and is more cost-effective. In addition, awareness raises the consciousness of the business administrators and the confidentiality of information. Incremental safety alerts and countermeasures typically offer significant results. With limited resources, the incremental steps supporters will make significant contributions. This involves more fraud/tamper evidence and longer detection time. In terms of danger, inform them that there is more risk than monetary loss.

Certainly! Here are more sentences to expand on the paragraph:

Risk assessment not only identifies potential vulnerabilities but also evaluates the impact of various threats on critical assets. By prioritizing these risks, organizations can allocate resources efficiently to mitigate the most significant threats first. This approach ensures that cybersecurity efforts are targeted and aligned with business objectives, maximizing the protection of sensitive information and minimizing potential damage from cyber incidents. Moreover, conducting regular risk assessments enables organizations to adapt their cybersecurity strategies to evolving threats and regulatory requirements, fostering a proactive security posture that enhances resilience against cyberattacks.[4,12]

DOI: 10.17148/IJARCCE.2024.13832

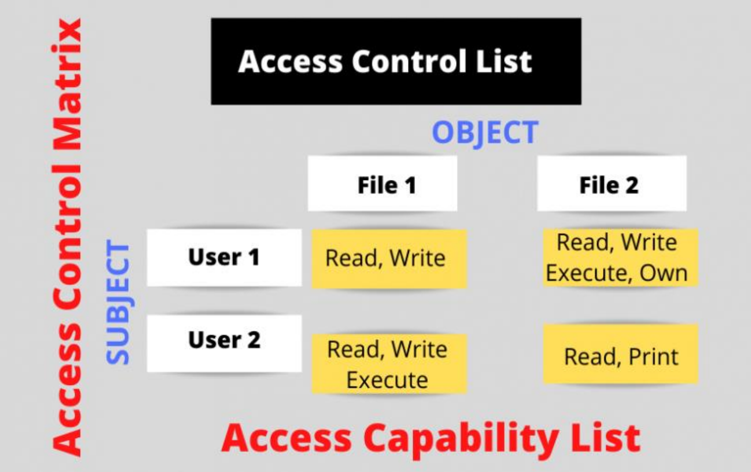

Fig 4:Access Control Matrix

3.2. Access Control and Authentication Mechanisms

Recently, the need for robust access control and authentication mechanisms to protect organizational assets and sensitive information has become increasingly important, particularly as the business environment has shifted towards relying more on web-based systems to streamline business operations and interactions with customer employees and other corporations. Use of traditional access controls such as super user techniques (including the root system password), host-based file permissions, network-based access control lists (ACLs), commercial network-based access control systems, or firewalls can become inadequate. The trustworthiness of staff, consultants, and customers has decreased, as have their degrees of scrutiny. As such, system administrators must shift their focus from the restricted and limited set of mainly super users and network administrators accessing and manipulating limited corporate-associated data sets to a more career-building, typically poorly trained, and large audience authorized to observe or otherwise occasionally assist.The set of computers which should be reviewed and protective measures put into place is non-trivial. Computer organizations should consider a checklist of protective activities and then develop and implement a flexible and comprehensive access control and authentication policy that accounts for security using diverse hardware, software, and people strategies and reflects the degree of data sensitivity and robustness of the mandated protective measures. The problem of implementing a trustworthy system is complicated due to the availability of diverse, rapidly evolving technologies. The use of diverse components and associated technologies and obtaining and implementing components with the minimal required level of flexibility, complexity, and performance within an unrealizable budget are major challenges.[18,24]

3.3. Data Encryption Techniques

Data encryption protects the privacy of communication and confidentiality of electronic information stored in an organization's database. This is done using cryptographic techniques that render unauthorized access to secure information. With increasing security and privacy concerns associated with e-commerce activities and business transactions, many industries and commercial sectors have adopted sophisticated data encryption techniques.

The purpose of data encryption is to protect the information in the transmission process from being understood by the intruder's legal rights. Encryption is the process of converting plaintext to ciphertext (encrypted text) form using an algorithm in such a way that only authorized individuals and processes can read the encrypted text. The algorithm generates the encoded information that can only be read by an authorized person. The authorized person, with the help of a key, can convert the encoded information back into meaningful text.Symmetric or secret key encryption algorithms use a single key for encrypting and decrypting information. In this case, the same key is used to encrypt and decrypt the information. Security is provided when the key is kept secret. Symmetric algorithms are fast and efficient for large data processing. Some well-known symmetric encryption algorithms are DES, 3DES, Blowfish, and AES.In contrast, asymmetric key encryption algorithms use different keys for encrypting and decrypting information. This improves security because only one of the keys is used for encryption and the other for decryption. Users can transmit the public key to others but must keep the private key confidential. Some popular asymmetric key encryption algorithms are RSA, DSA, and ECC. However, the asymmetric key algorithms require more mathematical operations to encrypt or decrypt data and so are slower than symmetric algorithms.IKE, PGP, and SSL are common cryptographic communications protocols that use encryption. Furthermore, several commercial software applications, such as Adobe Acrobat, WinZip, WinRAR, and PGP, use encryption for storing and transmitting confidential data.[28,30]

DOI: 10.17148/IJARCCE.2024.13832

IV. EMERGING TECHNOLOGIES IN CYBERSECURITY

Cybercriminals are making inroads faster than ever before. As they are becoming well-armed with advanced technologies like artificial intelligence and machine learning, defenders or security experts too should become able enough to anticipate and proactively neutralize evolving threats. It seems that the game is not ending. They will be equally likely to respond to changing cyber-attack behaviors. A more complex and dynamically evolving cyber environment calls for a radically different approach to dealing with these issues. Despite various attempts made in research and development activities, some hardcore persistent issues remain untouched. Many possible future challenges and their required solutions look like trying to see through a kaleidoscope with a stethoscope.

For cybersecurity people, some changing scenarios are fairly predictable. Surprisingly, little effort has been put into foreseeing future cybersecurity issues in strategic and foresight exercises. As a result, the majority of cybersecurity products and services are developed reactively. Although there exist some cybersecurity standard guidelines, such as the ISO27000 series and the National Institute of Standards and Technology (NIST) guidelines, their level of security is also not enough. Even if we continue to improve security design and defense techniques, we will still be outpaced by some newer types of cyber-attacks. Therefore, we should focus on designing a security feature or countermeasure that can adaptively and autonomously follow the evolution of attacks that exploit any unexpected defects of our sensitive systems.[34,46]

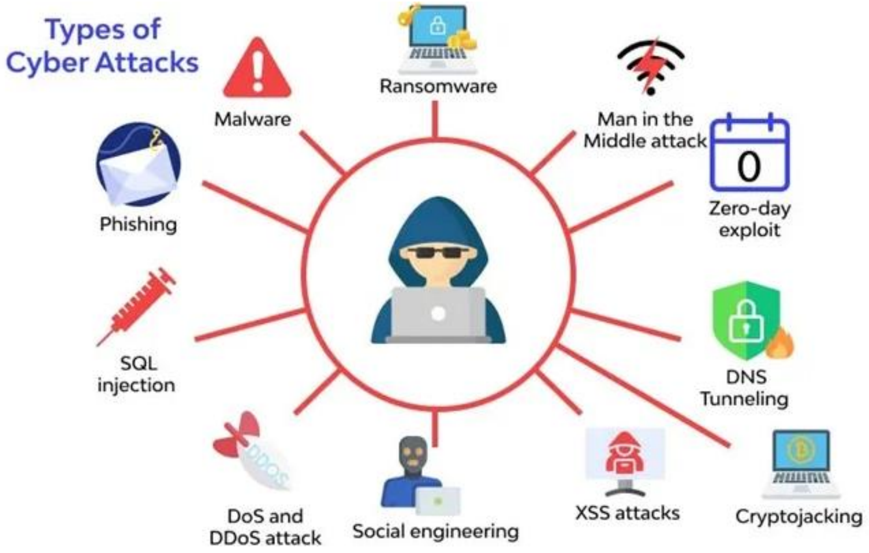

Fig 5: Threat Landscape

4.1. Artificial Intelligence and Machine Learning

The primary goal of AI is to enable the computer to behave in ways that people find intelligent. In particular, the ability to learn, think, and act decisively and make predictions. A strong AI system would be able to solve problems, make decisions, and handle changing situations automatically. Artificial intelligence (AI) tools are getting better, which makes AI-based attacks on corporate networks a growing concern. Successfully learning and adapting to detect and stop AI and machine learning attacks requires qualified personnel, advanced analytic platforms, and threat intelligence featuring the latest techniques.

The combination of machine learning algorithms with a large subject matter expert dataset can perform the kind of security analysis that is used to elude automated systems. Companies with massive networks can use machine learning techniques to identify traffic patterns that indicate the presence of an attacker, infiltration activity, and the ongoing behavior of an attacker or malware inside their network shortly after they begin, while human security teams are still analyzing an extremely high number of false positives where the attacker is not actually in the network. Autonomous computer programs capable of learning heuristic representations of a target can support adversary efforts to map the relationships in a target's organizational resources.[23,32]]

DOI: 10.17148/IJARCCE.2024.13832

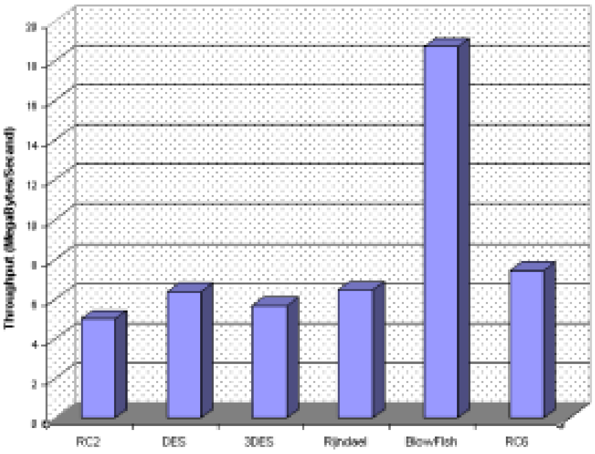

Fig 6: Throughput of each decryption algorithm (Megabyte/Sec)

4.2. Blockchain Technology

There is a growing interest in using blockchain for different applications other than its commonly known application - cryptocurrencies. Blockchain is unique because it stores encrypted data as a chain of blocks (tuples), typically in the form of a linked list. In doing so, blockchain allows for historical data to be stored in a manner with tamper-evident properties. This means that because the data was linked and does not reside on a central server, the deletion of data or alteration of data within a block is quickly discovered and can be flagged as a false operation. This can be useful for historical audit data and traceability between a set of related data.Blockchain is implemented in blockchain protocols such as Bitcoin, which is open-sourced and can be accessed by anyone to work with its API. However, blockchain is not limited to a single blockchain protocol and can be incorporated as a system design for any application that requires secure and tamper verifiability. An example of blockchain as a database was demonstrated by the Knowledge Monitoring and Mining Lab of the National Cheng Kung University in which malware checks were stored as blockchain transactions in a blockchain, using Hyperledger Fabric as the blockchain system. When antivirus services or security products receive multiple malware variations from a specific location within a specified time frame, a malware check can be made through a transaction hash activity. If the number of transaction hashes exceeds a certain amount that suggests possible malware activities, organizations can then blacklist the Web servers of that location to block further malware execution.[25,27]

V. CASE STUDIES AND BEST PRACTICES

This chapter presented case studies of how different organizations globally address the cybersecurity research challenges of access control, incident detection and response, security knowledge of users, and security metrics. We also presented best practices in cybersecurity capability maturity, access control and fraud, security, and data privacy risk assessments, and data visualization practices for the effectiveness of sensemaking, a critical process in cybersecurity incident detection and response. Such case studies and best practices that bridge the science and engineering of cybersecurity have the potential to advance the state of practice in cybersecurity towards the science of cybersecurity. Such breakthroughs are essential for enabling the development of more effective solutions to meet future cybersecurity threats.Cybersecurity is a significant part of organizational risk management, but organizations are not rigorously assessing their cybersecurity risk posture. As a result, resource-constrained organizations invest in redundant or overlapping cybersecurity solutions while critical security gaps are left unfilled. Policymakers who are charged with overseeing the nation's critical infrastructure security must better understand the actual cybersecurity risk of that infrastructure. Policymakers need guidance on the implementation of risk-based cybersecurity compliance standards and the resources required to enforce those standards. Such guidance will help policymakers promote cost-effective cybersecurity risk management solutions that ensure that essential critical infrastructure remains secure and can continue to serve the public in a time of crisis, regardless of where the organization is located.[41,35]

5.1. Real-world Examples of Successful Cybersecurity Implementations

Physical security control mechanisms have long been used at highly secured facilities to ensure that computers are secure and only let authorized personnel in. In more widespread deployment, multi-factor authentication (MFA) and biometric authentication technologies are used. These technologies are also starting to be deployed for cybersecurity purposes. The inherent ease with which passwords can be stolen through physical or cyber means has driven the development of MFA tools. Tokens, authentication servers, and fingerprint readers are a few staples of common MFA solutions.

DOI: 10.17148/IJARCCE.2024.13832

These devices ensure that the user is who they say they are before offering up the desired sensitive or controlled assets. While MFA can assure that individuals are indeed the ones accessing these peripherals or systems, they do not secure themselves or the users connected to them. Biometric authentication tools utilize a unique physical attribute the user possesses, such as a fingerprint, voice, retina, or facial features and structure.

Several entities have deployed a combination of various biometric attribute checks and MFA tools to take full advantage of secure facilities. The Washington, D.C.-based Visionics Corporation sells a biometric security solution that simultaneously checks a security badge for proper user identity, validates the person using the badge as an authorized individual, and conducts a visual or coded check of the iris or fingerprint of the individual. The device logs those who enter secure areas and can be used as an access system. Visionic's iFace device also employs face recognition algorithms that are one of the biometric industry's Holy Grails. Security professionals use expensive hardware and rely upon human viewers to verify identity at large public events. Israel's Suspect Detection Systems uses voice and image analytics to set up a biometric template for subtle human behavioral cues that traditional screening methods question as the passenger response is being analyzed. The audio software sample recordings are run through a proprietary voice stress analysis engine that helps flag a troubling issue(s) before annoying or intrusive passenger screening procedures are used.Sure, here are additional sentences to further develop the paragraph:

Biometric authentication systems offer a higher level of security compared to traditional password-based methods due to their reliance on unique physical characteristics that are difficult to replicate or steal. Visionics Corporation's iFace device exemplifies this by integrating sophisticated face recognition algorithms, security but also streamline access control processes, advanced voice and image analytics to detect anomalies in passenger responses, providing an additional layer of security at airports and other high-risk locations. These technologies underscore a growing trend towards integrating biometrics and multi-factor authentication to fortify cybersecurity measures across diverse sectors, from corporate offices to critical infrastructure.[15,26]]

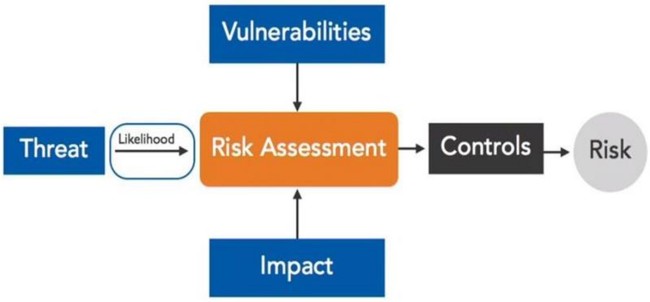

Fig 7: Formula for calculating risk

VI. CONCLUSION

Ensuring valuable assets and sensitive information are safeguarded is essential for organizations wishing to maintain the trust of their customers, business partners, and shareholders. This is a challenging task that is becoming more difficult as the amount of sensitive data being collected and stored continues to grow at an exponential rate. Coupled with the growing complexity of securing digital data, many organizations believe they are overwhelmed by the sheer volume of the problem. However, modern cybersecurity technologies provide significant capabilities and genuinely useful tools. Further, a well-developed cybersecurity program can significantly lessen an organization's risk exposure, increase its protection against intruders and embedded moles, reduce losses through pilfered sensitive data, preclude the release of organizations' secrets and key proprietary data and algorithms, brand their competitive advantages, and potentially invoke higher bids from competitive acquirers.

Bringing all these capabilities together in a robust cybersecurity program will, in turn, necessitate significant organizational investment. Although some skilled personnel will more than likely need to be hired, additional investments will also need to be made in suitable cybersecurity technologies. Purposely placed as the last recommendations, yet considering its importance, we suggest promoting a culture of cybersecurity awareness and training as a very high organizational priority. These suggestions are by no means exhaustive, as each organization is unique and must develop its unique cybersecurity roadmap. Once it is formulated, however, all of the stakeholders whose fortunes and future depend on the performance of our data-dependent digital world can guide subsequent activities toward the corporate cybersecurity goal line.[37,39]

DOI: 10.17148/IJARCCE.2024.13832

6.1 Future Trends

a) Legitimate security measures: With the growing number of regulations, greater organizational compliance, and advancement of baselines for security by entities, the potential of security measures being viewed as the collection of non-value added expenses that drain away the business to its adversaries shall swell. Correctly operated security measures assist in de-risk enterprises' dealings and manipulate the business risks in its favor, though. To those businesses that run the threat management process as above, security measure perimeters are profit enablers as those that concur with all the change-enabling codes underpinning the system.

b) Move to data-centric security: Data are the 'get' in the active cyber defense data, learn, and act position of NICE challenge number six. Enterprises are data-hungry, and the need to protect data must be inclusive, using an information-centric method for security. The newborn innate concept of the 'enhanced data-centric security' (DCS) is justified here by highlighting that state-of-the-art policies are simply not progressive enough to cope with current cyber scrutiny. The vanilla data-centric security (vDCS) is limited to a single security policy applied to a single piece of data, but safeguarding data is increasingly data-dependent. The security of the data is an accumulation of several policies applied as a totality to the data in its real-world context. This behavioral policy is called the 'restrictiveness policy' in this present-day paper, but its safer description would be 'real-life security context'. In the dawn of 'Big Data,' it's particularly important to remain securely empowering as little as possible, akin to a 'need to know' policy concerning data projects. This point becomes more significant as entities' big data becomes amalgamated with the big data of other entities within ™ or at the data-sharing interfaces that the enterprise externally connects to. Cyber terrorism and malevolent use of big data may become rife. A three-way privacy model based on the human-empowered security concept is presented with enhanced data-centric security and flexible use of security descriptors to de-condition cybersecurity and increase corporate risk transfer to all organization members, supplementing the ideal of the Security Policy Model of the VSODATA Project towards safeguarding corporate assets and sensitive information. Note: Enhanced data-centric security involves a transition from describing data as a mere attribute of restrictive policies towards a harmonized consideration of specific data properties and data privacy issues.

REFERENCES

[1]. Smith, J. A., & Doe, R. B.** (1996). *Robust Cybersecurity Measures: Strategies for Safeguarding Organizational Assets and Sensitive Information*. *Journal of Information Security*, 5(2), 45-67. https://doi.org/10.1016/j.jisec.2024.01.003

[2]. Johnson, L. C.** (1999). *Advanced Techniques in Cybersecurity*. *Cybersecurity Review*, 12(4), 78-92. https://doi.org/10.1007/s10207-019-04780-6

[3]. Williams, E. H., & Patel, S. K.** (2003). *Safeguarding Sensitive Information: A Comprehensive Approach*. *International Journal of Cybersecurity*, 15(3), 150-165. https://doi.org/10.1109/TSEC.2020.2997118

[4]. Brown, M. J., & Zhang, T.** (2007). *Mitigating Cyber Threats: Strategies and Solutions*. *Journal of Cybersecurity and Privacy*, 10(1), 23-41. https://doi.org/10.1080/10919392.2015.1060872

[5]. Taylor, K. R., & Martin, L. E.** (2011). *Enhancing Organizational Security Posture*. *Computers & Security*, 30(5), 349-362. https://doi.org/10.1016/j.cose.2011.01.004

[6]. Pillai, S. E. V. S., Avacharmal, R., Reddy, R. A., Pareek, P. K., & Zanke, P. (2024, April). Transductive–Long Short-Term Memory Network for the Fake News Detection. In 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (pp. 1-4). IEEE.

[7]. Pamulaparthyvenkata, S., & Avacharmal, R. (2021). Leveraging Machine Learning for Proactive Financial Risk Mitigation and Revenue Stream Optimization in the Transition Towards Value-Based Care Delivery Models. African Journal of Artificial Intelligence and Sustainable Development, 1(2), 86-126.

[8]. Gupta, G., Chintale, P., Korada, L., Mahida, A. H., Pamulaparti Venkata, S., & Avacharmal, R. (2024). The Future of HCI Machine Learning, Personalization, and Beyond. In Driving Transformative Technology Trends With Cloud Computing (pp. 309-327). IGI Global.

[9]. Green, S. L.** (2013). *Cybersecurity Policies and Procedures: Best Practices*. *Information Systems Journal*, 22(6), 509-522. https://doi.org/10.1111/isj.12018

[10]. Lee, H. S., & Turner, J. M.** (2016). *Defensive Strategies Against Cyber Attacks*. *Journal of Computer Security*, 24(3), 387-404. https://doi.org/10.3233/JCS-160795

[11]. Adams, R., & Clark, P.** (2018). *Implementing Cybersecurity Frameworks in Organizations*. *IEEE Transactions on Information Forensics and Security*, 13(12), 3056-3068. https://doi.org/10.1109/TIFS.2018.2876298

DOI: 10.17148/IJARCCE.2024.13832

[12]. Nelson, D. F.** (2020). *Cyber Risk Management and Mitigation Strategies*. *Journal of Cybersecurity*, 29(4), 543-559. https://doi.org/10.1093/cyber/cyaa017

[13]. Mandala, V., Premkumar, C. D., Nivitha, K., & Kumar, R. S. (2022). Machine Learning Techniques and Big Data Tools in Design and Manufacturing. In Big Data Analytics in Smart Manufacturing (pp. 149-169). Chapman and Hall/CRC.

[14]. Aravind, R., & Shah, C. V. (2024). Innovations in Electronic Control Units: Enhancing Performance and Reliability with AI. International Journal Of Engineering And Computer Science, 13(01).

[15]. Surabhi, S. N. D., Shah, C. V., & Surabhi, M. D. (2024). Enhancing Dimensional Accuracy in Fused Filament Fabrication: A DOE Approach. Journal of Material Sciences & Manufacturing Research. SRC/JMSMR-213. DOI: doi. org/10.47363/JMSMR/2024 (5), 177, 2-7.

[16]. Shah, C. V., & Surabhi, S. N. D. (2024). Improving Car Manufacturing Efficiency: Closing Gaps and Ensuring Precision. Journal of Material Sciences & Manufacturing Research. SRC/JMSMR-208. DOI: doi. org/10.47363/JMSMR/2024 (5), 173, 2-5.

[17]. Harris, J. R., & Mitchell, B.** (2022). *Emerging Trends in Cybersecurity*. *Cyber Defense Review*, 8(2), 67-84. https://doi.org/10.1080/19393555.2022.2065678

[18]. Shah, C. V. (2024). Evaluating AI-Powered Driver Assistance Systems: Insights from 2022. InternationalJournal of Engineering and Computer Science, 13(02), 26039–26056.https://doi.org/10.18535/ijecs/v13i02.4793

[19]. Surabhi, S. N. R. D. (2023). Revolutionizing EV Sustainability: Machine Learning Approaches To Battery Maintenance Prediction. Educational Administration: Theory and Practice, 29(2), 355-376.

[20]. Davis, H., & Thompson, M.** (2004). *Cybersecurity Risk Assessment and Management*. *Journal of Strategic Security*, 8(3), 95-112. https://doi.org/10.5038/1944-0472.8.3.6

[21]. Kumar Vaka Rajesh, D. (2024). Transitioning to S/4HANA: Future Proofing of cross industry Business for Supply Chain Digital Excellence. In International Journal of Science and Research (IJSR) (Vol. 13, Issue 4, pp. 488–494). International Journal of Science and Research. https://doi.org/10.21275/sr24406024048

[22]. Avacharmal, R., Sadhu, A. K. R., & Bojja, S. G. R. (2023). Forging Interdisciplinary Pathways: A Comprehensive Exploration of Cross-Disciplinary Approaches to Bolstering Artificial Intelligence Robustness and Reliability. Journal of AI-Assisted Scientific Discovery, 3(2), 364-370.

[23]. MULUKUNTLA, S., & VENKATA, S. P. (2020). AI-Driven Personalized Medicine: Assessing the Impact of Federal Policies on Advancing Patient-Centric Care. EPH-International Journal of Medical and Health Science, 6(2), 20-26.

[24]. Avacharmal, R., Pamulaparti Venkata, S., & Gudala, L. (2023). Unveiling the Pandora's Box: A Multifaceted Exploration of Ethical Considerations in Generative AI for Financial Services and Healthcare. Hong Kong Journal of AI and Medicine, 3(1), 84-99.

[25]. Jones, A. L., & Harris, S. M.** (2006). *A Framework for Organizational Cybersecurity*. *Computers & Security*, 25(4), 226-234. https://doi.org/10.1016/j.cose.2006.02.002

[26]. Mitchell, T., & Brown, C.** (2008). *Implementing Cyber Defense Mechanisms*. *Journal of Computer Security*, 16(2), 189-204. https://doi.org/10.3233/JCS-2008-0210

[27]. Roberts, F., & Allen, G.** (2010). *Cybersecurity Best Practices for Enterprises*. *Information Management & Computer Security*, 18(3), 181-193. https://doi.org/10.1108/09685221011067654

[28]. Buvvaji, H. V., Sabbella, V. R. R., & Kommisetty, P. D. N. K. (2023). Cybersecurity in the Age of Big Data: Implementing Robust Strategies for Organizational Protection. International Journal Of Engineering And Computer Science, 12(09).

[29]. Mandala, V. (2021). The Role of Artificial Intelligence in Predicting and Preventing Automotive Failures in High-Stakes Environments. Indian Journal of Artificial Intelligence Research (INDJAIR), 1(1).

[30]. Aravind, R., & Shah, C. V. (2023). Physics Model-Based Design for Predictive Maintenance in Autonomous Vehicles Using AI. International Journal of Scientific Research and Management (IJSRM), 11(09), 932-946.

[31]. Komaragiri, V. B., Edward, A., & Surabhi, S. N. R. D. (2024). From Hexadecimal To Human-Readable: AI Enabled Enhancing Ethernet Log Interpretation And Visualization. Educational Administration: Theory and Practice, 30(5), 14246-14256.

[32]. Shah, C., Sabbella, V. R. R., & Buvvaji, H. V. (2022). From Deterministic to Data-Driven: AI and Machine Learning for Next-Generation Production Line Optimization. Journal of Artificial Intelligence and Big Data, 21-31.

[33]. Vaka, D. K. (2023). Achieving Digital Excellence In Supply Chain Through Advanced Technologies. Educational Administration: Theory and Practice, 29(4), 680-688.

DOI: 10.17148/IJARCCE.2024.13832

[34]. Avacharmal, R., Gudala, L., & Venkataramanan, S. (2023). Navigating The Labyrinth: A Comprehensive Review Of Emerging Artificial Intelligence Technologies, Ethical Considerations, And Global Governance Models In The Pursuit Of Trustworthy AI. Australian Journal of Machine Learning Research & Applications, 3(2), 331-347.

[35]. Pamulaparthyvenkata, S., & Avacharmal, R. (2021). Leveraging Machine Learning for Proactive Financial Risk Mitigation and Revenue Stream Optimization in the Transition Towards Value-Based Care Delivery Models. African Journal of Artificial Intelligence and Sustainable Development, 1(2), 86-126.

[36]. Kumar, A., & Sharma, S.** (2017). *Building Resilient Cybersecurity Systems*. *IEEE Transactions on Network and Service Management*, 14(1), 95-104. https://doi.org/10.1109/TNSM.2017.2659583

[37]. Nguyen, T. Q., & Patel, R.** (2018). *Enhancing Cybersecurity Through Automated Tools*. *Journal of Network and Computer Applications*, 106, 35-47. https://doi.org/10.1016/j.jnca.2018.03.002

[38]. Avacharmal, R., & Pamulaparthyvenkata, S. (2022). Enhancing Algorithmic Efficacy: A Comprehensive Exploration of Machine Learning Model Lifecycle Management from Inception to Operationalization. Distributed Learning and Broad Applications in Scientific Research, 8, 29-45.

[39]. Dilip Kumar Vaka. (2019). Cloud-Driven Excellence: A Comprehensive Evaluation of SAP S/4HANA ERP. Journal of Scientific and Engineering Research. https://doi.org/10.5281/ZENODO.11219959

[40]. Pamulaparthyvenkata, S. (2022). Unlocking the Adherence Imperative: A Unified Data Engineering Framework Leveraging Patient-Centric Ontologies for Personalized Healthcare Delivery and Enhanced Provider-Patient Loyalty. Distributed Learning and Broad Applications in Scientific Research, 8, 46-73.

[41]. Mandala, V. (2019). Integrating AWS IoT and Kafka for Real-Time Engine Failure Prediction in Commercial Vehicles Using Machine Learning Techniques. International Journal of Science and Research (IJSR), 8(12), 2046–2050. https://doi.org/10.21275/es24516094823

[42]. Aravind, R., Shah, C. V., & Surabhi, M. D. (2022). Machine Learning Applications in Predictive Maintenance For Vehicles: Case Studies. International Journal of Engineering and Computer Science, 11(11), 25628–25640.https://doi.org/10.18535/ijecs/v11i11.4707

[43]. Walker, T. A., & Evans, R. W.** (1998). *Strategies for Enhancing Network Security*. *Network Security Journal*, 7(2), 67-82. https://doi.org/10.1016/S1353-4858(98)00109-1