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 journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121016

Regulatory Landscape in Cyber security: Framework, Criteria, and Guiding Principles

Beerappa Belasakarge[1], Dr. Basavaraj G N[2], Dr. Usha B A[3]

Department of Cyber Security, B M S Institute of Technology & Management, Bengaluru, India[1]

Asst. Professor, Department of Information Science & Engineering, B M S Institute of Technology & Management, Bengaluru, India[2]

Professor, Department of ISE, BMS Institute of Technology and Management[3]

Abstract: Cybersecurity pertains to safeguarding systems linked via the Internet, including hardware, software, and data, shielding them against cyber attacks from malicious actors. A regulatory framework for cybersecurity becomes essential to safeguard information technology and computer systems, compelling a variety of organizations and businesses to defend their data and systems against online attacks. Viruses, phishing, Trojan horses, worms, Denial-of-Service (DoS) attacks, unauthorized access (such the theft of personal data or intellectual property), and control system intrusions are examples of potential cyberattacks.

Our emphasis in this paper is on illustrating the value of various standards in bolstering cyber defense and explaining the structure of cyber security frameworks. Detailed discussions revolve around the array of security threats, attack methodologies, and countermeasures prevalent in the realm of cyber security. Furthermore, we delve into the challenges pertaining to standardization within the cyber security domain. Additionally, a thorough exploration of the national cyber security strategy, designed to secure digital landscapes, and various government policies aiming to ensure cyber security, is presented. The discussion is concluded with important recommendations that are vital to the fields of digital safety and cyber defense.

Keywords: Framework, Cyber Security, Cyber Attacks, Policies

I. INTRODUCTION

There has been a rising trend in recent years that focus on cybersecurity in the field of study. Cybersecurity involves avoiding unwanted access by intruders or attackers to information systems, including hardware, software, infrastructure, and the data and services they deliver. Harm or misuse of these systems can occur intentionally or accidentally, leading to breaches in security protocols.

A 2016 review highlighted the need for increased regulation or incentives to enhance cyber risk management across services that are absolutely necessary, like vital national infrastructure. The concern was driven by the rising threat of cyberattacks, which might have profound effects for consumer confidence, public safety, and economic growth. For instance, the amount of Internet banking fraud cases rose by 64% in 2015 to £133.5 million. with criminals increasingly targeting businesses and high-net-worth individuals.

Changes in mobile banking have also been discussed, with an emphasis on the risks involved and recent malware attacks. Solutions to secure mobile banking have been explored, particularly in the context of user authentication challenges and their potential solutions.

This section emphasizes the significance of criteria for cyber defense and information security. These standards serve critical purposes, impacting how we approach information security globally and within different communities. The development of these standards is driven by several important reasons, and they play a pivotal role in shaping and improving our strategies for safeguarding information and defending against cyber threats across diverse geographical regions and communities.

1.1 The Importance of Standards in Cyber Defense and Information Security.

In this section, we delve into the significance of having standards in the fields of information security and cyber defense. The development and implementation of these standards are driven by several crucial reasons, and they have a profound impact on how we approach and enhance information security on a global scale and within various communities.

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 journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121016

Here are the key reasons for the development of these standards, which serve to improve information security practices across different regions and communities:

- **Enhancing Efficiency and Effectiveness:** Standards help streamline and optimize important processes related to information security and cyber defense, making them more efficient and effective.
- **Enabling Integration and Interoperability:** They facilitate The combination of systems and ensure interoperability, allowing different technologies and systems to work together seamlessly.
- **Comparing Products and Methods:** Standards provide a basis for comparing different products or methods, making it easier to assess their relative strengths and weaknesses.
- **Evaluation of New Products/Services:** Users can use standards as a means to evaluate the performance and suitability of new products and services in the realm of information security.
- **Guiding Technology and Business Model Deployment:** Standards provide a structured approach for deploying new technologies and business models, ensuring a systematic and secure implementation.
- **Simplifying Complex Environments:** In complex and dynamic environments, standards simplify the management and maintenance of information security measures.
- **Promoting Economic Growth:** By establishing common standards, these initiatives can stimulate economic growth, as they ensure fairness for businesses and promote innovation in the discipline of cyber defense and information security.

1.2. Foundational Cybersecurity Requirements: The Minimum Standard

"Minimum Cybersecurity Standard" refers to a set of fundamental requirements and practices that organizations or individuals must adhere to in order to establish a basic level of security for their digital assets and information. This standard serves as a foundation for safeguarding against cyber threats and ensuring the data and system availability, integrity, and secrecy. Some key points related to the minimum cybersecurity standard include:

- **Basic Security Measures:** It entails implementing essential security measures, such as strong password policies, regular software updates, and antivirus protection, to protect against common cyber threats like malware and unauthorized access.
- **Data Encryption:** The standard often includes encrypting sensitive data both in transit and at rest to prevent unauthorized access and data breaches.
- **Access Control:** It involves restricting access to systems and data, ensuring that only authorized individuals can access and modify information.
- **Incident Response:** Organizations should have a plan in place for detecting, responding to, and mitigating cybersecurity incidents, ensuring minimal damage and downtime.
- **Employee Training:** Educating employees about cybersecurity best practices is a crucial component of this standard, as human error is a common entry point for cyberattacks.
- **Regular Auditing and Monitoring:** Continuous monitoring and periodic security audits help identify vulnerabilities and ensure compliance with the minimum cybersecurity standard.
- **Compliance with Legal and Regulatory Requirements:** Organizations may need to align their cybersecurity practices with relevant laws and regulations, depending on their industry and location.
- **Patch Management:** Keeping software, operating systems, and applications up-to-date with security patches is essential for protecting against known vulnerabilities.
- **Data Backup and Recovery:** Regularly backing up data and having a reliable recovery plan is critical to ensure business continuity if there is a loss of data or ransomware attacks.
- **Third-Party Vendors:** Organizations should extend cybersecurity standards to third-party vendors and partners with whom they exchange information or work together to guard against external vulnerabilities.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023
DOI: 10.17148/IJARCCE.2023.121016

In essence, the minimum cybersecurity standard establishes a baseline of security measures that all entities should follow to protect themselves and their digital assets from cyber threats. It is a proactive approach to reducing the risk of cybersecurity incidents and their potential negative consequences.

1.3. Key Research Contribution.

This article makes several significant contributions:

- It outlines and investigates cyberattacks, security requirements, and preventative methods.
- The article delves into the framework for managing cyber security incidents and its various uses.
- It addresses the difficulties posed by uniformity in the area of computer security.
- The paper offers perceptions regarding international strategy for enhancing cyberspace security and various government policies related to this.
- Lastly, it offers essential recommendations pertinent to both cyber security and cyber defense.

1.4. Outline of the Paper

The article's organization is structured as follows:

Section 2: This section is dedicated to detailing cyber attacks, security requirements, and measures.
Section 3: It focuses on discussing the cyber security incident management framework.
Section 4: The challenges associated with standardization in the realm of cyber security are explored.
Section 5: This section concentrates on strategic objectives aimed at securing cyberspace.
Section 6: Various government policies related to cyber security are provided.
Section 7: Essential recommendations pertaining to both cyber security and cyber defense are presented.

The article concludes in Section 8.

Section 2: Cyber attacks, security requirements, and measures

In this part, the article commences by examining different types of cyber attacks carried out by adversaries (attackers). It then proceeds to delve into the security prerequisites and countermeasures essential for safeguarding against these cyber threats.

2.1. Cyber attacks: The section goes on to discuss various cyber attacks perpetrated by adversaries, shedding light on some of these attack types.

- **Diverse Attack Types:** Cyber attacks encompass a wide range of tactics and techniques employed by malicious actors, often referred to as adversaries or attackers.
- **Vulnerability Exploitation:** Attackers use flaws in software, networks, or computer systems to gain unwanted access or disrupt operations.
- **Common Attack Methods:** Some common cyber attack methods include malware infections, phishing attempts, ransomware attacks, denial of service (DoS) attacks, and data breaches.
- **Malware:** Malware is malicious software designed to infiltrate systems, steal data, or cause damage. Examples include worms, viruses, spyware and Trojans.
- **Phishing:** Phishing attacks involve tricking individuals into revealing sensitive information, often through deceptive emails or websites.
- **Ransomware:** Ransomware encrypts a victim's data, and attackers demand a ransom for decryption keys, making data inaccessible until payment is made.
- **Denial of Service (DoS):** In DoS attacks, the aim is to overwhelm a system or network with excessive traffic, rendering it unavailable to users.
- **Data Breaches:** Unauthorized access to sensitive information is a data breach. potentially leading to its theft or exposure.

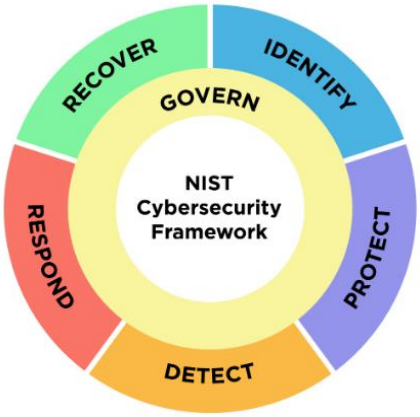
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.102 ⁜ Peer-reviewed journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121016

- **(APTs) Advanced persistent threats :** APTs are sophisticated, long-term cyber attacks often conducted by nation-state actors or well-funded organizations.
- **Social Engineering:** Attackers may trick people into disclosing sensitive information through social engineering technique or performing actions that compromise security.
- **Zero-Day Exploits:** Zero-day exploits target not yet recognized vulnerabilities or patched, making them highly valuable to attackers.



NIST cybersecurity framework.

Ransomware: Ransomware is a software that encrypts files or even the entire computer system making it impossible to access. Cyber attackers then demand a payment in cryptocurrency in exchange, for providing the decryption key. Ransomware attacks can cause damage to businesses and individuals who heavily rely on their data. Its generally advised against paying the ransom as it doesn't guarantee the retrieval of data. Can encourage further attacks.

Spyware: Spyware is a kind of software that operates covertly by monitoring and collecting information from a users computer or device without their knowledge or consent. This information may include keystrokes, browsing history, login credentials and personal data. Typical uses of spyware include identity theft, espionage or targeted advertising. Detecting and removing spyware is important to safeguard ones privacy and security.

Unauthorized Access: Unauthorized access refers to gaining entry into a computer system, network or data without authorization or permission. It poses a cybersecurity threat that often occurs due to passwords misconfigured security settings or exploiting vulnerabilities. Unauthorized access can result in data breaches, theft of information or inflict damage, on computer systems.
Ensuring protection, from access requires the implementation of authentication methods, access restrictions and security protocols.

2.2 focuses on the essential requirements for ensuring cybersecurity

Certainly, here is a description of the provided cyber security requirements:

Confidentiality (Privacy): This requirement emphasizes that data in computer networks, especially information from various organizations and sources, should only be accessible to authorized individuals. It ensures that sensitive data remains confidential and protected against unauthorized access.

Integrity: The integrity requirement states that information from different organizations and sources must not be altered or tampered with by unauthorized entities, such as attackers. It guarantees the integrity of the data. and unaltered during transmission and storage within a network.

Authentication : A method for confirming a user's identity is authentication. Only approved account holders will be able to access their accounts, thanks to this. Depending on the level of security required, authentication can involve single-factor, two-factor, or multi-factor authentication. For example, in two-factor authentication, a user uses two types of credentials, like a password and a smart card, for login. Multi-factor authentication, on the other hand, uses three different kinds of authentication, including a smart card, password, and personal biometric like fingerprint and iris scans.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023
DOI: 10.17148/IJARCCE.2023.121016

Biometrics offer advantages such as being difficult to forget, share, copy, distribute, or guess, making them more secure compared to traditional passwords.

Availability: This requirement focuses on protecting information systems are protected against Denial of Service (DoS) attacks, allowing users to access or log in to the system whenever they need to without disruptions.

Authorization: Authorization grants specific permissions to individuals, allowing them to perform authorized and legal activities within a system. It restricts users from accessing information beyond what they are allowed based on their defined roles in the system.

Physical Theft of Devices: Adversaries sometimes physically seize devices, particularly in the context of the Internet of Things (IoT), which is made up of a variety of smart devices. It is essential to protect against physical theft in order to stop unauthorized access and improper use of these gadgets.

1. Identify (Cyber Security Governance):

- Clear Responsibility: Departments must designate individuals responsible for the security of sensitive data and key operational services.
- Management Policies: Implement appropriate management policies and processes to guide overall cybersecurity efforts.
- Risk Management: Identify and manage significant risks related to sensitive information and services.
- Supplier Assurance: Ensure that external suppliers meet cybersecurity standards, potentially requiring them to demonstrate cybersecurity adherence or hold a valid cyber essentials certificate.
- Training and Awareness: Provide training and guidance to accountable individuals, promoting a culture of cybersecurity awareness.

2. Protect (Access Control):

- Access Control: Allow access to sensitive information and services only for authorized and authenticated users or systems.
- User and System Identification: Users and systems must be identified and authenticated before accessing information or services.

3. Detect (Cyberattack Detection):

- Event Capture: Capture events that can be used with threat intelligence to detect known threats.
- Defining Protection Needs: Clearly define what must be protected and monitor for indicators of unwanted situations.
- Monitoring Adaptation: Adapt monitoring solutions to align with changing business and technology environments and evolving threats.
- Attack Detection: Ensure that attackers using common cyberattack techniques are detected.
- Transactional Monitoring: Implement transactional monitoring for digital services susceptible to cybercriminal activity.

4. Respond (Incident Response):

- Incident Response Plan: Develop a detailed incident response plan with clear actions, roles, and responsibilities.
- Communication: Establish communication plans for incidents, including notification to relevant authorities and bodies.
- Legal Compliance: obey the law's requirements for reporting personal data breaches.
- Testing and Mitigation: Regularly test the incident response plan and apply mitigation measures promptly after an incident.
- Post-Incident Learning: Analyze incident lessons learned and include them in upcoming versions of the incident management plan.

5. Recover (Continuity of Operations):

- Contingency Mechanisms: Identify and test contingency measures to ensure the continuity of essential services in case of failure or compromise.
- Service Restoration: Ensure well-practiced scenarios for restoring services to normal operation after an incident.
- Post-Incident Recovery: Apply lessons learned from post-incident recovery activities to enhance the technical protection of systems or services and address systemic vulnerabilities.

Additionally, the text also mentions security concepts like confidentiality (ensuring data is only accessible by authorized individuals), integrity (preventing unauthorized alterations to data), authentication (verifying user identity), non-

DOI: 10.17148/IJARCCE.2023.121016

repudiation (preventing users from denying actions), freshness (ensuring the timeliness of data), and the importance of protecting IoT smart devices from physical capture and misuse.

2.3 discusses the actions and precautions taken to enhance cybersecurity.

Here's a description of the presented cyber security measures and solutions:

Firewalls: Firewalls are essential security components with three common types: packet filters, application-level gateways, and circuit-level gateways. The primary goals of a firewall include channeling all traffic through it, allowing only authorized traffic based on defined security policies, and ensuring the firewall itself is resilient. Following these goals helps prevent cyberattacks.

Anti-virus Software: Anti-virus software has evolved through four generations. First-generation relies on virus signatures, while second-generation uses heuristic rules for detection. Third-generation software recognizes viruses by their activities rather than their structure and is memory-resident. Multiple anti-virus methods are packaged in fourth-generation software. Updated antivirus software is essential for defending systems from threats.

(IDS/IPS) Intrusion Detection System and Prevention Systems : Intrusion detection systems (IDS) detect suspicious activities in a network or system, including intrusions and misuse. Intrusion prevention systems (IPS) not only recognize but also stop attacks. While IDS can raise alarms, IPS can block malicious traffic. Having both IDS and IPS is vital for network and system security.

Encryption: Data stored in servers should be encrypted to prevent unauthorized access. Encryption can use symmetric key (e.g., 3DES and AES) or public key mechanisms (e.g., ECC and RSA), depending on the application.

Login Credentials: Users should use high-entropy passwords to strengthen authentication and reduce the risk of offline password guessing attacks. Strong authentication methods, such as biometrics, can also be employed.

Awareness: Awareness programs are essential to educate users and employees about potential threats like phishing, malware, and malicious downloads. Promoting proper authentication practices and the use of good antivirus software is crucial.

Operating System Updates: Keeping the operating system up-to-date is crucial for security. Software manufacturers constantly monitor bugs and hazards, providing remote fixes via the internet for connected systems. Up-to-date operating systems enhance reliability, security, and performance.

Architecture of Cybersecurity Incident Management Framework (CIMF): The CIMF architecture consists of three main components: technology infrastructure, security operations center, and computer emergency response center. It aims to achieve primary objectives, including preventing cybersecurity incidents, minimizing their impact on confidentiality, integrity, and availability, and reducing threats and dangers as incidents occur. The architecture plays a vital role in managing and responding to cybersecurity incidents effectively.

4.1. Challenges within the organization's structure and operation.

Standard Development Organizations (SDOs) have proliferated over the past ten years. These organizations were largely founded by diverse industries, including well-known ones like the World Wide Web Consortium (W3C), Adobe, Open Data Center, Internet Engineering Task Force (IETF), and Oasis. The large time and human commitments required by conventional SDOs like the European Telecommunications Standards Institute (ETSI) and the International Telecommunication Union (ITU) might be considered as a partly industry reaction to the rise in SDOs.

4.2. Domains of standardization

During the process of creating standards, only specific distinct areas are taken into account. Here are some of these areas:
- Diverse technical benchmarks.
- Different metrics primarily associated with business objectives.
- Various definitions.
- Various facets linked to organizational aspects.

It's important to highlight that some sections within the standards end up being excessively standardized. Only a limited number of standards focus on ensuring compliance with privacy and data protection protocols.

DOI: 10.17148/IJARCCE.2023.121016

4.3. Absence of flexibility.

The procedure of formulating and reaching a consensus on different standards is time-consuming, ranging from a few months (in the most efficient scenarios) to several years. It's crucial for standards to advance at a similar pace; otherwise, they may become outdated or only partially relevant to real-world settings. To address this issue, it is necessary to implement "good practice" documents as preliminary steps to the standards. Consequently, well-developed good practice documents can serve as a foundation for a corresponding standard once they have reached an adequate level of maturity.

4.4. Competition among Standards:

In the realm of information and cybersecurity, various groups set standards across different areas. These standards may vie with each other for adoption, making it challenging for end-users to discern which standard best suits their specific needs. Additionally, standards from different families may be combined to achieve particular objectives. For example, in implementing Public Key Infrastructure (PKI), organizations often blend standards like X.509 from the International Telecommunication Union (ITU) for certificate format, PKIX from IETF for primary PKI, and Public Key Cryptography Standards (PKCS) like RSA for secure device interfacing.

4.5. Economic Factors:

Certain providers see their use of proprietary standards as a unique advantage. However, there are cases where companies, despite their dominant position, fail to effectively support and implement standards for their products. A pertinent example is the diverse charger plugs used by mobile phone vendors, causing inconvenience and resource wastage. To address this, the European Union (EU) mandates a universal mobile phone charger plug to enhance customer convenience. Companies in influential positions may find incentives to adopt interoperable standards, as it can bolster competition. Employing proprietary standards can have advantages, such as locking consumers in. This lock-in process can occur in two ways: customers may be unable to buy or merge compatible products from multiple competitors, generating more revenue for providers, and it can be inconvenient for customers to switch to another supplier due to the complexities of moving data and processes.

4.6. Lack of Awareness:

Despite the drawbacks associated with proprietary standards, there are instances where customers, including those in government organizations, do not actively demand open standards. Therefore, raising awareness among customers is an important task.

5. National Cybersecurity Strategy:

The national strategy for securing cyberspace identifies three strategic objectives: preventing cyber attacks on critical infrastructure, reducing national vulnerability to such attacks, and minimizing damage and recovery time from cyber attacks that do occur. To achieve these objectives, the strategy outlines five national priorities, including developing a response system, reducing threats and vulnerabilities, increasing awareness and training, securing government cyberspace, and establishing a system of national and international cyberspace security cooperation.

The strategy encourages companies to regularly review their technology security plans and individuals to configure firewalls and install antivirus software. Additionally, it promotes the creation of a federal center to track, identify, and evaluate cyberattacks, as well as to boost cybersecurity research and enhance government-industry coordination.

6. Government Policies:

6.1. Federal Government:

The federal government has proposed several cybersecurity regulations focusing on specific industries. These include the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm–Leach–Bliley Act of 1999, and the Homeland Security Act of 2002, which encompasses the Federal Information Security Management Act (FISMA). These regulations apply to healthcare organizations, financial institutions, and federal agencies, mandating them to protect their systems and information.

However, these regulations do not cover certain computer-related industries like Internet Service Providers (ISPs) and software companies. They also do not specify the implementation details of cybersecurity measures. Bruce Schneier, founder of Cupertino's Counterpane Internet Security, argues that companies may not invest enough in cybersecurity without government enforcement.

The Data Quality Act empowers the Office of Management and Budget with statutory authority to enact crucial infrastructure protection regulations through the Administrative Procedure Act rule-making process. This idea requires further assessment and legal analysis before rule-making can commence.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023
DOI: 10.17148/IJARCCE.2023.121016

6.2. State Governments:

State governments play a role in enhancing cybersecurity by increasing public awareness of firms with weak security measures. In 2003, California passed the Notice of Security Breach Act, which requires companies holding personal information of California residents to disclose details of security breaches. This includes information like names, driver's license numbers, social security numbers, and financial information.

In 2004, the California State Legislature enacted Assembly Bill 1950, which applies to businesses that possess or maintain personal information for California residents. This regulation mandates businesses to uphold a reasonable level of security and extend security practices to business partners. It represents an improved version of the federal standard, but still requires a reasonable level of cybersecurity.

6.3. Cybersecurity National Security Action Plan

In 2016, former U.S. President Barack Obama introduced the Cybersecurity National Security Action Plan (CNAP). This plan aimed to promote information sharing about security events among private sector entities and the government. It outlined long-term strategies to safeguard the U.S. against cyber threats, focusing on issues like raising public awareness about cybercrime risks, enhancing cybersecurity measures, safeguarding personal information, and educating people on digital security. One notable aspect was the establishment of a diverse commission to provide recommendations for stronger cybersecurity in both public and private sectors. Additionally, the plan emphasized upgrading Government IT for enhanced security and advocated for a 35% increase in cybersecurity investments compared to 2016.

6.4. Cybersecurity Strategies of Non-EU Nations

This section introduces the cybersecurity strategies of three non-European Union (EU) countries, namely the United States, Canada, and Japan. Several other countries, including India, Australia, New Zealand, and Colombia, have also formulated their own National Cyber Security Strategies (NCSS), highlighting the global recognition of cybersecurity's importance.

6.4.1. United States of America

The U.S. released its international strategy for cyberspace in May 2011, outlining activities across seven interconnected areas. These areas involve collaborative efforts between the government, international partners, and the private sector, focusing on promoting international standards and open markets, enhancing network security, extending collaboration in law enforcement, preparing for various security challenges, advocating for effective internet governance structures, aiding in international development, and supporting fundamental freedoms and privacy.

6.4.2. Canada

Canada's cybersecurity strategy, published in 2010, rests on three pillars: securing government systems, partnering to secure vital cyber systems beyond the federal government, and assisting Canadians in staying secure online. The first pillar concentrates on defining roles and responsibilities to fortify the security of federal cyber systems and raise awareness across the entire government. The second pillar encompasses collaborative initiatives with provinces, territories, private sector, and critical infrastructure sectors. The third pillar addresses combating cybercrime and protecting Canadian citizens in online environments, with a particular emphasis on privacy concerns.

6.4.3. Japan

Japan's cybersecurity strategy, established in May 2010, encompasses key actions in areas like reinforcing policies against potential cyber-attacks, adapting to changes in the information security landscape, and implementing proactive information security measures.

6.5. China's Cybersecurity Services

KPMG, with extensive experience in cybersecurity advisory services, possesses a deep understanding of China's cybersecurity landscape and regulatory requirements. They offer various advisory services based on customer needs, covering strategy and governance, security transformation, cyber defense services, and assessments and assurance.

6.6. ePrivacy Regulation

The ePrivacy regulation proposes rules for safeguarding privacy in electronic communications. It applies to any business providing online communication services, using online tracking technologies, or engaging in electronic direct marketing. This regulation seeks to establish high-level privacy standards for all electronic communications, including new players, stricter rules on communications content and meta-data, business opportunities, simplified cookie rules, protection against spam, and more effective enforcement.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.102 ⁜ Peer-reviewed journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023
DOI: 10.17148/IJARCCE.2023.121016

II. CONCLUSION

First, we covered a variety of cyberattacks and their security.

requirements as well as answers. After that, we talked about the CIMF (Cyber Security Incident Management Framework). The CIMF should intentionally make it possible for each organization to actively take part in a coordinated national cyber crisis response, it was determined. After then, we talked about a number of standardized issues that are important for cyber security. An industry standard for cyber security includes things like tools, security principles, different types of policies, security protection, risk management, training, etc. Various government initiatives and the national strategy for cyberspace security were also covered. Finally, we offered a few suggestions that are helpful for both cyber protection and security.

REFERENCES

[1] R.J. Deibert, R. Rohozinski, Risking security: policies and paradoxes of cy-berspace security, International Political Sociology 4 (1) (2010) 15–32.
[2] UK Government Policies, Tech. rep., 2016. http://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf.
[3] M. Wazid, S. Zeadally, A.K. Das, Mobile banking: Malware threats and secu-rity solutions, IEEE Consumer Electron. Mag., http://dx.doi.org/10.1109/MCE. 2017.2764115.
[4] A. Chang-Gu, NIST-Cyber Security Framework, 2018, https://p16praetorian. com/blog/nist-cybersecurity-framework-vs-nist-special-publication-800-53.
[5] G.N. Ericsson, Cyber security and power system communication—essential parts of a smart grid infrastructure, IEEE Trans. Power Deliv. 25 (3) (2010) 1501–1507. J. Srinivas et al. / Future Generation Computer Systems 92 (2019) 178–188 187
[6] W. Knowles, D. Prince, D. Hutchison, J.F.P. Disso, K. Jones, A survey of cyber security management in industrial control systems, Int. J. Crit. Infrastruct. Prot. 9 (2015) 52–80.
[7] The Minimum Cyber Security Standard, Tech. rep., 2019. http: //assets.publishing.service.gov.uk/government/uploads/system/uploads/ attachment_data/file/719067/25062018_Minimum_Cyber_Security_ Standard_gov.uk_3.pdf.
[8] Chronology of Data Breaches, 2010. http://web.archive.org/web/ 20100613183200. http://www.privacyrights.org/ar/ChronDataBreaches. htm. (Accessed on 2018).
[9] List of Common Malware Types, http://www.malwaretruth.com/the-list-of-malware-types/. (Accessed on 2018).
[10] A. Ginter, Cyber Security Review, http://www.cybersecurity-review.com/ industry-perspective/control-system-security-attack-models/). (Accessed on 2018).
[11] H. Mun, K. Han, Y.S. Lee, C.Y. Yeun, H.H. Choi, Enhanced secure anonymous authentication scheme for roaming service in global mobility networks, Math. Comput. Modelling 55 (1) (2012) 214–222.
[12] Q. Xie, B. Hu, X. Tan, M. Bao, X. Yu, Robust anonymous two-factor authen-tication scheme for roaming service in global mobility network, Wirel. Pers. Commun. 74 (2) (2014) 601–614.
[13] D. Zhao, H. Peng, L. Li, Y. Yang, A secure and effective anonymous authenti-cation scheme for roaming service in global mobility networks, Wirel. Pers. Commun. 78 (1) (2014) 247–269.
[14] I. Memon, I. Hussain, R. Akhtar, G. Chen, Enhanced privacy and authentication: an efficient and secure anonymous communication for location based service using asymmetric cryptography scheme, Wirel. Pers. Commun. 84 (2) (2015) 1487–1508.
[15] A.G. Reddy, A.K. Das, E.J. Yoon, K.Y. Yoo, A secure anonymous authentication protocol for mobile services on elliptic curve cryptography, IEEE Access 4 (2016) 4394–4407.
[16] C.T. Li, C.C. Lee, C.Y. Weng, A chaotic maps based key agreement and user anonymity protocol without using smart cards and symmetric key en/decryptions, J. Internet Technol. 18 (5) (2017) 975–984.
[17] C.T. Li, C.C. Lee, C.Y. Weng, A secure three party node authentication and key establishment scheme for the internet of things environment, J. Internet Technol. 19 (1) (2018) 147–155.
[18] C.T. Li, C.-L. Chen, C.C. Lee, C.Y. Weng, C.M. Chen, A novel three-party password-based authenticated key exchange protocol with user anonymity based on chaotic maps, Soft Comput. 22 (8) (2018) 2495–2506.
[19] J. Srinivas, A.K. Das, N. Kumar, J. Rodrigues, Cloud Centric Authentication for Wearable Healthcare Monitoring System, IEE Trans. Dependable Secure Comput. http://dx.doi.org/10.1109/TDSC.2018.2828306.
[20] D. Mishra, A.K. Das, S. Mukhopadhyay, A secure user anonymity-preserving biometric-based multi-server authenticated key agreement scheme using smart cards, Expert Syst. Appl. 41 (18) (2014) 8129–8143.
[21] Y. Lu, L. Li, X. Yang, Y. Yang, Robust biometrics based authentication and key agreement scheme for multi-server environments using smart cards, PLoS One 10 (5) (2015) 1–13.

DOI: 10.17148/IJARCCE.2023.121016

[22] H. Lin, F. Wen, C. Du, An improved anonymous multi-server authenticated key agreement scheme using smart cards and biometrics, Wirel. Pers. Commun. 84 (4) (2015) 2351–2362.
[23] D. He, D. Wang, Robust biometrics-based authentication scheme for multi-server environment, IEEE Syst. J. 9 (3) (2015) 816–823.
[24] C. Wang, X. Zhang, Z. Zheng, Cryptanalysis and improvement of a biometric-based multi-server authentication and key agreement scheme, PLoS One 11(2) (2016) 1–25.
[25] V. Odelu, A.K. Das, A. Goswami, A secure biometrics-based multi-server au-thentication protocol using smart cards, IEEE Trans. Inf. Forensics Secur. 10 (9) (2015) 1953–1966.
[26] M. Wazid, A.K. Das, V. Odelu, N. Kumar, W. Susilo, Secure Remote User Authenticated Key Establishment Protocol for Smart Home Environment, IEEE Trans. Dependable Secure Comput., http://dx.doi.org/10.1109/TDSC.2017.2764083.
[27] C.T. Li, M.S. Hwang, An efficient biometrics-based remote user authentication scheme using smart cards, J. Netw. Comput. Appl. 33 (1) (2010) 1–5.
[28] A.K. Das, Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards, IET Inf. Secur. 5 (3) (2011) 145– 151.
[29] A.K. Das, S. Zeadally, D. He, Taxonomy and analysis of security protocols for internet of things, Future Gener. Comput. Syst. 89 (2018) 110–125.
[30] EPIC Bill Track Tracking Privacy, Speech, and Cyber-Liberties Bills in the 111th Congress, 2010. http://www.epic.org/privacy/bill_track.html. (Accessed on 2018).
[31] W. Stallings, Cryptography and Network Security: Principles and Practices, third ed., Pearson Education, India, 2004.
[32] Advanced Encryption Standard (AES), fIPS PUB 197, National Institute of Standards and Technology (NIST), U.S. Department of Commerce, 2001. Avail-able at http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf. (Accessed on 2018).
[33] N. Koblitz, Elliptic curve cryptosystems, Math. Comp. 48 (1987) 203–209.
[34] R.L. Rivest, A. Shamir, L.M. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM 21 (2) (1978) 120–126.
[35] Cyber Incident Management Planning Guide, https://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf. (Accessed on 2018).
[36] S. Purser, Standards for Cyber Security, 2014.
[37] Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cy-berspace, European Commission, 2013. http://eeas.europa.eu/archives/docs/ policies/eu-cybersecurity/cybsec_comm_en.pdf.
[38] DHS, The National Strategy to Secure Cyberspace, 2003.
[39] M.T. McCaul, America is under cyber attack: Why urgent action is needed, http://homeland.house.gov/sites/homeland.house.gov/files/04-24-12%20McCaul%20Open.pdf.
[40] J. Garamone, Defense.gov News Article: Panetta Spells Out DOD Roles in Cyberdefense, 2012. http://archive.defense.gov/news/newsarticle.aspx?id= 118187.
[41] B. Levinson, Do Agencies Already Have the Authority to Issue Critical In-frastructure Protection Regulations? 2016. http://www.circleid.com/posts/ 20120820_agencies_authority_to_issue_critical_infrastructure_protection/.
[42] L.A. Gordon, M.P. Loeb, W. Lucyshyn, R. Richardson, 2005 CSI/FBI Computer Crime and Security Survey, 2005.
[43] Executive order – improving critical infrastructure cybersecurity, The White House, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/ 02/12/executive-order-improving-critical-infrastructure-cybersecurity.
[44] FACT SHEET: Cybersecurity National Action Plan, 2016. http: //obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan. (Accessed on 2018).
[45] European union agency for network and information security (enisa), national cyber security strategies, 2012. https://www.enisa.europa.eu/publications/ cyber-security-strategies-paper.
[46] H.A. Schmidt, Launching the u.s. international strategy for cyberspace, 2011. https://obamawhitehouse.archives.gov/blog/2011/05/16/launching-us-international-strategy-cyberspace.
[47] Canada's cyber security strategy : for a stronger and more prosperous canada, 2010. http://publications.gc.ca/site/eng/379746/publication.html.
[48] Japan's cyber security strategy, 2018. http://www.nisc.go.jp/eng/.
[49] Overview of china's cybersecurity law, 2017. https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf.
[50] Europa.eu, ePrivacy Regulation on Europa.eu, 2016. http://ec.europa.eu/ digital-single-market/en/proposal-eprivacy-regulation.

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 journal / Refereed journal ⁜ Vol. 12, Issue 10, October 2023

DOI: 10.17148/IJARCCE.2023.121016

BIOGRAPHY

Beerappa Belasakarge-

Beerappa Belasakarge, born on December 1st, 1997, in the historic city of Bidar, Karnataka, is a distinguished figure in the field of cybersecurity. His profound knowledge and extensive experience have established him as a trusted authority in the realm of digital security.

With a relentless passion for safeguarding digital landscapes, Beerappa embarked on a journey of higher education, culminating in a Bachelor's degree in Electronics and Communication Engineering followed by a Master's degree in Cyber Security . These academic pursuits laid a solid foundation for his future endeavors.

Beerappa's commitment to excellence and his insatiable curiosity led him to Rooman Technologies Pvt. Ltd., where he currently serves as a Cyber Security Analyst. In this role, he has consistently demonstrated an exceptional ability to identify vulnerabilities and implement robust security measures, ensuring the protection of critical digital assets for clients.

Beyond his role as an analyst, Beerappa is a dedicated Cyber Security Trainer, sharing his expertise with aspiring professionals. Through insightful workshops and hands-on training sessions, he imparts invaluable knowledge on the latest trends, threats, and best practices in the field of cybersecurity.

Beerappa's contributions to the cybersecurity community extend far beyond his professional duties. He is a vocal advocate for cybersecurity awareness and has actively participated in initiatives aimed at educating individuals and organizations about the importance of digital security.

In recognition of his exemplary work, Beerappa has received accolades within the industry, affirming his status as a thought leader and innovator in the realm of cybersecurity. His dedication to continuous learning and staying at the forefront of emerging technologies is evident in his ongoing pursuit of certifications and professional development opportunities.

Outside of his professional commitments, Beerappa is known for his collaborative spirit and willingness to mentor aspiring cybersecurity professionals. He believes in the power of knowledge-sharing and actively engages with the broader cybersecurity community through conferences, seminars, and online forums.

With a clear vision for the future of cybersecurity, Beerappa Belasakarge remains a beacon of inspiration for both seasoned professionals and those just starting their journey in this critical field. His tireless dedication to securing digital landscapes and empowering others underscores his status as a true luminary in the world of cybersecurity.