IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.301

Volume 3, Issue 5, June 2023

Cyber Security

Sanjana M S[1], Mohammad Muneeb[2], Ranjith[3]

Guide and Assistant Professor, Department of Computer Science and Engineering[1]
Students, Department of Computer Science and Engineering[2]
Alva's Institute of Engineering and Technology, Mangalore, India

Abstract*: The Internet, a loose global network of connections held networks has facilitated the transfer of data and information between many networks. information and Security concerns have grown significantly over the past few years due to the transmission of information between networks at different locations. A small number of people have also exploited the internet for illegal operations like frauds and unauthorised access to other people's networks. Cybercrimes are the name given to these illegal online actions. These days, we frequently hear the term in the news due to the rising popularity of online activities like online banking, online shopping, etc. Therefore, "Cyber Law" was developed in order to deter and punish the cybercriminals. Cyberlaw is the branch of the legal system that deals with the Internet, cyberspace, and other legal matters like online privacy or online security. It is also referred to as "law of the web". In order to provide a brief overview of what cybercrime is, the perpetrators of cybercrime hackers and crackers, various forms of cybercrimes, and the evolution of cyberlaws in India, this chapter is organised into various sections with the aims in mind. The chapter also discusses the numerous preventive measures that can be employed to stop this "hi-tech" crime in India as well as how these laws function.*

Keywords: Power Factor, Power Factor Transducer, Power Quality, microcontroller (AT89S52/C51), Capacitors

I. INTRODUCTION

The rapid growth of technology has created a lot of opportunities and conveniences in today's connected and digital society. However, technology has also brought forth previously unheard-of difficulties, particularly in the area of cybersecurity. Strong cybersecurity measures are urgently needed given the rise in cyberthreats and attacks that have caused worries about the security and integrity of digital systems. The importance of cybersecurity in the face of increasing threats is stressed by the authors of a seminal study by Scarfone, K., & Mell,

P. (2013) titled "Cybersecurity Challenges: Threats, Vulnerabilities, and Mitigation Strategies". By offering a thorough analysis of cybersecurity and looking at its importance, essential ideas, changing dangers, and new trends, this review paper intends to build upon and expand the insights offered in Scarfone and Mell's work.

- Importance of Cybersecurity: The crucial necessity of cybersecurity is highlighted by the growing reliance on digital infrastructure and the rising level of sophistication of cyberattacks. The potential repercussions of poor cybersecurity measures, which can include monetary losses, compromised privacy, reputational damage, and even threats to national security, must be understood by organisations, governments, and individuals. To effectively reduce risks and protect the digital environment, it is crucial to promote a thorough awareness of cybersecurity.
- Key Concepts and Frameworks: Examining the major theories and frameworks that form the basis of cybersecurity is crucial to understanding its complexity. Core components like risk assessment, threat modelling, vulnerability analysis, and incident response will all be covered in this examination. It will also go through well-known frameworks that give organisations an organised way to handle cybersecurity risks, like the NIST Cybersecurity Framework, ISO 27001, and the CIS Controls.
- Evolving Cyber Threat Landscape: Since cyber dangers are dynamic and ever- changing, being proactive is essential to avoiding being taken advantage of by bad actors. In this overview, common attack vectors like malware, phishing, ransomware, and social engineering will be examined. Additionally, it will go over newly discovered dangers like supply chain attacks, Internet of Things (IoT) vulnerabilities, and AI-driven assaults.

DOI: 10.48175/568

For the purpose of creating efficient defences and implementing effective countermeasures, it is essential to comprehend the changing threat landscape.

- Emerging Trends and Technologies: New trends and technologies are shaping the cybersecurity landscape as technology continues to advance. This assessment will examine cutting-edge strategies that have the potential to improve cybersecurity procedures, including machine learning, behavioural analytics, and blockchain. The expanding significance of cloud security, mobile device security, and the interaction of cybersecurity with cutting-edge technologies like 5G networks and edge computing will also be covered.
- Regulatory and Compliance Considerations: Promoting cybersecurity practises and upholding compliance are important tasks for governments and regulatory organisations. The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), among others, will be examined in depth in this section of the evaluation along with their effects on cybersecurity procedures. Additionally, it will examine the difficulties and chances brought forth by shifting regulatory environments.

II. DEFINITION

Preventing harm to, safeguarding, and restoring computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its accessibility, integrity, authentication, confidentiality, and nonrepudiation.

III. EXAMPLES

- Obtaining credit card data fraudulently.
- Accessing the official website
- Internet and email fraud.
- Identity theft.
- Data theft and sales from businesses.
- Ransomware attacks.
- Cyberextortion (demanding money to stop a threatened attack).
- Cyber espionage, in which hackers get access to private or public data.
- Crypto jacking, in which hackers mine bitcoin using resources that they do not control.

IV. HISTORY

The development of the internet, technological developments, and the appearance of fresh cyber threats have all had an impact on the history of cybersecurity. Here is a synopsis of cybersecurity's past along with some references for more research:

The Morris Worm (1988) was one of the first well-known instances of a pervasive computer worm that infected thousands of machines on the early internet. The Morris Worm was developed by Robert Tappan Morris. The need for more stringent security measures was brought to light by this occurrence.

Formation of the Computer Emergency Response Team (CERT) (1988): In response to the Morris Worm incident, Carnegie Mellon University founded the Computer Emergency Response Team (CERT). In order to coordinate responses to incidents involving computer security and to encourage cooperation among diverse stakeholders, CERT was extremely important.

Growing Threats from the Internet in the 1990s: The growing use of the internet created fresh security difficulties. The emergence of computer viruses, hacking, and denial-of-service assaults are examples of how cyberthreats have changed. In order to lessen these hazards, antivirus software and firewall technologies emerged at this time.

The Y2K scare, which brought attention to possible weaknesses in computer systems owing to the date rollover, led to increased investments in cybersecurity (1999–2000). Organisations realised the importance of taking strong security precautions to safeguard vital infrastructure and avoid interruptions.

Critical infrastructure was the target of a number of high-profile cyber-attacks in the 2000s, including attacks on government networks, financial systems, and power grids. Notable occurrences include the distributed denial-of-service

(DDoS) assaults on Estonia and Georgia and the Stuxnet worm, which targeted industrial control systems. These accidents confirmed how crucial it is to protect vital infrastructure from online assaults.

Nation-State Attacks and Advanced Persistent Threats (2010s): Advanced persistent threats (APTs), which are sophisticated cyberattacks usually conducted by nation-state actors for espionage or sabotage goals, increased in the 2010s. Attacks on Sony Pictures, the Office of Personnel Management (OPM), and the WannaCry ransomware outbreak are notable examples.

V. TYPES OF CYBER CRIME

5.1 Malware Attacks

An instance of a malware attack occurs when malicious software, also referred to as malware, is used to break into a computer system or network, disrupt operations, or steal sensitive data. Attacks by malware are a major worry in today's digital world since they can seriously harm people, businesses, and even entire countries.

The WannaCry ransomware outbreak in May 2017 moved quickly over the world, infecting tens of thousands of machines in more than 150 nations. It took advantage of a flaw in the Windows operating system to encrypt files on affected computers and demand a Bitcoin ransom to decrypt them.

In June 2017, there was yet another significant malware attack that mostly targeted Ukrainian organisations while also spreading to other nations. Not Petya, which was previously thought to be ransomware, was eventually found to be a malicious wiper software. For the affected businesses, it resulted in extensive disruption and financial losses.

The software development process of SolarWinds, a well-known provider of IT management software, was found to have been penetrated in December 2020 as a result of a sophisticated supply chain attack. A malicious backdoor was included into software updates by threat actors as a result of the attack, giving them unauthorised access to the systems of several organisations, including government institutions and significant technological firms.

The Colonial Pipeline, which provides petroleum to the eastern United States, was the target of a ransomware assault in May 2021. The attack, which resulted in a temporary suspension of the pipeline and created fuel shortages in numerous regions, was carried out by the Dark Side ransomware organisation.

These illustrations demonstrate the serious effects that malware assaults may have on vital systems, organisations, and people. To lessen the likelihood of such assaults, they stress the significance of strong cyber security measures, such as frequent software patching, network segmentation, employee awareness training, and strong access controls. To protect against ever- evolving malware threats, it's essential to remain diligent and knowledgeable about the most recent security procedures.

A. Viruses

In terms of cybersecurity, the term "virus" refers to a particular kind of malware that attacks computer systems and spreads by joining forces with trustworthy programmes or files. In the field of cybersecurity, viruses have posed a serious threat by corrupting data, destabilising computer systems, and jeopardising the safety of both people and businesses.

B. Trojans

refers to a particular kind of malicious software that uses legal software or files to conceal its true identity while doing unauthorised actions on a computer system. Trojan horses pose a serious risk because they give attackers the ability to access restricted areas, steal confidential data, or inflict other types of harm.

C. Worms

In the field of cybersecurity, worms refer to a type of malicious software (malware) that can self-replicate and spread across computer networks without requiring user interaction. Worms typically exploit vulnerabilities in operating systems or applications to propagate and carry out various malicious activities.

DOI: 10.48175/568

D. Botnets

In the context of cybersecurity, a botnet is a collection of compromised computers or other devices that are managed by a single attacker or central authority. These compromised computers, often known as "bots" or "zombies," are frequently infected with malware and are capable of being remotely directed to engage in hostile behaviour. Botnets are frequently used for distributed denial-of-service (DDoS) assaults, spam email distribution, data theft, virus distribution, and other online criminal activities.
We can encounter malware if we have os vulnerabilities or if we download some l legitimate software from somewhere or we have some email attachments that were compromised with.

5.2 Phishing

Phishing is a type of cyberattack in which perpetrators assume the identity of trustworthy organisations or institutions in order to trick victims into disclosing sensitive information, including usernames, passwords, credit card numbers, or other personal information. Phishing assaults often take place through phoney emails, instant messaging, or websites that look like reliable sources, tricking unsuspecting people into divulging their personal data.

- Planning: To customise their phishing emails or messages, attackers investigate their targets and acquire data. They may obtain information from public sources about the target's company, position, or personal characteristics.
- Spoofing: Phishers frequently pose as reliable organisations, including well- known businesses, financial institutions, or governmental bodies. In order to trick their targets, they imitate the appearance and feel of legal communication channels, such as email addresses, website URLs, or even phone numbers.
- Baiting: Phishing assaults frequently use psychological ploys called "baiting" to lure victims. Attackers instill a sense of urgency or panic in their victims, making promises of rewards or threatening dire consequences in an effort to get them to act without fully assessing the situation.
- Delivery: Phishing emails or messages are distributed to numerous prospective victims using a variety of techniques. Mass spam email campaigns, personalised spear phishing emails, or even harmful adverts or social media posts are examples of this.
- Exploiting Trust: Phishers rely on people's faith in well-respected institutions to their advantage. To make their correspondence seem authentic, they could employ company branding, official logos, or email signatures. In order to deceive recipients into thinking the letter is authentic, they may also include private information or allusions that look real.
- Deception and Interaction: Phishing communications frequently ask recipients for sensitive data like account numbers, credit card information, or login passwords. This is called deception. Attackers may deceive users into opening malicious attachments or clicking on malicious links, which might result in more compromises.
- Data collection: When victims fall for the phishing scam, attackers take note of the information they have provided and can use it for a number of nefarious activities like identity theft, financial fraud, or unauthorised access to accounts or systems.

It's crucial to remember that phishing tactics are continually changing, and attackers are constantly honing their strategies to get past security precautions and take advantage of human weaknesses. Strong cybersecurity practises must be used by businesses and people, including email filtering, phishing awareness training for staff, regular software updates, and exercising caution when interacting with emails or other messages.

5.3 Password Attack

Password attacks are techniques used by cybercriminals to gain unauthorized access to user accounts or systems by exploiting weak passwords. These attacks target the vulnerability of poorly chosen or easily guessable passwords. Here are some common password attack methods in cybersecurity:

- Brute Force Attack: In a brute force attack, attackers repeatedly try all password combinations in hopes of finding the right one. This technique uses computers' computational capacity to quickly guess passwords by starting with straightforward and widely-used possibilities before moving on to more complicated ones.

- Dictionary Attack: This method of password guessing uses a list of words or phrases from dictionaries that are frequently used as passwords. Attackers speed through the process by attempting every word or phrase until a match is made. Dictionary assaults can be modified by giving dictionary words numerals or other special characters.
- Credential Stuffing: Using stolen username and password combinations from one website or a breach, attackers try them on numerous websites in a technique known as "credential stuffing." Users that use the same passwords across several accounts are the target of this attack, which gives the attacker access to unapproved accounts on other platforms.
- Phishing: Users might be duped into voluntarily disclosing their credentials through phishing assaults. Attackers trick victims into entering their login information on phoney websites made to seem like the real ones by sending them phoney emails or messages that appear to be legitimate but are actually false. Once the users have given their credentials, the attackers have the data and can access the system without authorization.

5.4 Distributed DoS Attack

A type of cyberattack known as a distributed denial of service (DDoS) assault involves the use of several compromised computers or other devices to systematically overload a target system, network, or website with traffic or requests. DDoS attacks try to stop the targeted resource from being available by using up all of its resources, such as bandwidth, computing power, or memory.

5.5 Man in the Middle Attack

Man-in-the-Middle (MitM) attacks are a sort of cyberattack in which an attacker deceives two parties into thinking they are directly speaking with each other by intercepting and maybe changing their communication. The information shared between the two parties is covertly relayed by the attacker, who may also modify it. An outline of a Man-in-the-Middle attack in cybersecurity is given below:

- Interception: The assailant places himself in the path of the two communicating parties and intercepts their communication. This can be accomplished via methods like ARP (Address Resolution Protocol) spoofing, exploiting holes in the network infrastructure, and compromising a router or switch.
- Communication Relay: After assuming the role of a middleman, the attacker now intercepts the messages being sent between the two parties. The attacker can either actively modify the communications before sending them to the intended recipient or passively eavesdrop on the conversation to make it seem as though it is unaffected.
- Data Modification: An attacker may occasionally change the intercepted data to suit their nefarious goals. This may entail changing the communications' contents, inserting malware or malicious code into the communication, or diverting traffic to malicious websites or servers.
- Bypassing Encryption: If the two parties' communication is encrypted, the attacker might try to undermine or get around the encryption in order to obtain the underlying data. This can be accomplished using bogus digital certificates, exploiting holes in the encryption protocols, or stealing the encryption keys.
- Impersonation: In some circumstances, the attacker might pretend to be one or both of the persons involved in the contact, leading each to believe they are speaking directly to the other. This can be especially useful for getting access to sensitive information.
- Impersonation: In some circumstances, the attacker might pretend to be one or both of the persons involved in the contact, leading each to believe they are speaking directly to the other. This is very useful for getting access to confidential information or login credentials..ation or qualifications.

A. PREVENTION OF MITM

Use encrypted Wireless Access Point (WAP) technology.
Constantly verify the connection's security. (HSTS or HTTPS)
Purchase a VPN.

DOI: 10.48175/568

DOWNLOAD ON THE GO: This assault takes place when unprotected machines become infected simply by browsing a website.

This attack has emerged as the main web security danger to be concerned about, according to findings from the most recent Microsoft Security Intelligence Report.

B. Rogue Software

Rogue software, commonly referred to as rogue security software or scareware, describes harmful apps or programmes that falsely assert to offer security protection or system optimisation but inadvertently damage the user's computer or make an attempt to swindle them. Rogue software pushes users to purchase a full version or do security-compromising activities by tricking them into thinking their machine is infected with malware or having other problems. An overview of malicious software in cybersecurity is given below:

- Distribution: Malicious websites, spam emails, deceptive marketing, and software downloads that are bundled with genuine ones are some of the common ways that rogue software is spread. Attackers utilise deception tactics to get people to download or install malicious software.
- Rogue software frequently replicates the appearance of real antivirus or system optimisation applications through deceptive interfaces. In order to instill a sense of urgency and dread in the user, they display scary messages, bogus scan results, or inflated security warnings.
- False Security Alerts: Once installed, malicious software produces false security alerts that falsely indicate that the user's computer is infected with malware or is having serious problems. These warnings are meant to persuade users to act and buy the malicious software's complete version.
- Unauthorised Changes: Malicious software may make unauthorised adjustments to the user's registry settings or system settings, which could compromise the stability or security of the system. They might disable reliable antivirus software or restrict access to websites that deal with security, making it challenging for consumers to get real help.
- Payment Scams: Malicious software frequently requests a licence payment or full version purchase from customers in order to fix the alleged security vulnerabilities. Even though the customer buys, the malicious software rarely offers any real security protection or resolves the reported issues.

VI. CYBER CRIME AND INFORMATION SECURITY

Use Secure Network Connections: When accessing sensitive information or engaging in online transactions, be careful to connect to secure and reliable networks. Do not use unsecured or public Wi-Fi networks for sensitive data-related tasks.

- Use dependable firewalls and security tools Install and keep up your devices' firewalls, antivirus programmes, and anti- malware solutions. To stay protected from the most recent dangers, keep them updated frequently.
- Attacks Using Social Engineering Techniques: Be wary of social engineering attacks using methods like phishing, pretexting, or baiting. Be wary of unauthorised emails, texts, or phone calls that ask for personal information or demand that you take immediate action.
- Regularly update and patch your software: Make sure your operating system, devices, and software are up to date with the most recent security patches and updates. Cybercriminals may take advantage of flaws in old software.
- Implement Strong Access Controls: Use strong passwords or passphrases and activate multi-factor authentication (MFA) whenever possible to implement tight access controls. By demanding additional verification outside of passwords, this adds an additional degree of protection.
- Secure Your Personal Devices: Set up strong PINs, patterns, or biometric locks on your laptops, tablets, and mobile devices to secure them. To protect your data in the event that your device is lost or stolen, turn on capabilities for remote tracking and wiping.
- Practice Safe Browsing: Use safe browsing techniques: Use caution when downloading files from websites. Avoid clicking on shady links, and before submitting any personal or financial information, be sure the website is legitimate.

DOI: 10.48175/568

- Regularly Back Up Your Data: Your vital data should be periodically backed up to an external hard drive, cloud storage, or a secure backup service. By doing this, you can be sure that your data can be restored in the event of a device crash or ransomware attack.
- Keep Up with Security dangers: Stay informed about the most recent frauds, attacks, and security dangers. To keep informed and take the required steps, follow reliable cybersecurity sources and organisations.

Educate Yourself and Others: Acquire knowledge on cybersecurity best practises and pass it along to loved ones, friends, and co-workers. To reduce the danger of cybercrime, foster a culture of cybersecurity awareness and alertness.

VII. CYBERSECURITY:

Cybersecurity is the activity of preventing unauthorised access to, use of, disclosure of, interruption of, alteration of, or destruction of computer systems, networks, and data. It entails putting policies and technologies in place to protect against online dangers and guarantee the privacy, accuracy, and accessibility of data.

Advantages:

- Protection against Cyber Attacks.
- Safeguarding Sensitive Data.
- Maintaining Business Continuity
- Protection of Reputation and Customer Trust.
- Compliance with Regulatory Requirements.

VIII. WHY DO WE NEED CYBERSECURITY?

Three main pillars of cyber security are:

Confidentiality: Confidentiality ensures that only authorised parties or institutions have access to sensitive information. Protecting data against unauthorised disclosure or access is involved. Confidentiality is maintained through measures including access limits, encryption, and secure communication protocols.

Integrity: Throughout its lifecycle, integrity makes ensuring that data is accurate, consistent, and unaffected. It entails guarding against unauthorised data change, deletion, or corruption. Data integrity can be preserved via methods like data validation, checksums, and digital signatures.

Availability: System, network, and data availability ensures that they are usable and accessible when required. It entails guarding against and lessening disturbances, outages, and denial-of- service assaults. Continuous availability is supported by redundancy, backup and recovery systems, and disaster recovery strategies.

IX. MOTIVES BEHIND CYBER CRIME

- Financial Gain
- Theft of Intellectual Property
- Espionage and Nation-State Attacks
- Hacktivism
- Personal Vendettas or Revenge

X. FAMOUS PEOPLE IN CYBER SECURITY

- In 1988, Robert T Morris was the first person to create internet worm.
- In 1990, Kevin Lee hacked telephone lines of KIIS-FM (Los Angeles).
- In 1999, David L Smith created Melissa virus.
- In 2004, Adam Botbyl gained unauthorized access to corporate computer network via and unsecured access points.

XII. DOMAINS IN CYBER SECURITY

- Security of the assets.
- Security engineering and architecture.
- Network security and communication.
- Management of identity and access.
- Security management.
- Assessment and testing of security.
- Security and software development.

XIII. CONCLUSION

In conclusion, cyber security is essential for safeguarding key infrastructure, securing confidential data, reducing financial losses, assuring business continuity, upholding trust, and complying with regulations. It is a crucial discipline that provides protection for people, businesses, and governments from the constantly changing range of cyberthreats, providing a safe and resilient digital environment.

XIV. ACKNOWLEDGMENT

In order to protect digital systems, data, and privacy, we are grateful to the committed experts and researchers in the field of cybersecurity. Their knowledge, creativity, and dedication to safeguarding our digital environment are crucial in fending off cyber dangers. We recognise their significant contributions and thank them for their efforts in guaranteeing the availability, confidentiality, and integrity of information.

REFERENCES

[1]. Scarfone, K., & Mell, P. (2013). Cybersecurity challenges: threats, vulnerabilities, and mitigation strategies. National Institute of Standards and Technology (NIST), U.S. Department of Commerce.
[2]. https://csrc.nist.gov/glossary/term/cybersecurity
[3]. https://www.irjet.net/archives/V9/i8/IRJET-V9I8255.pdf
[4]. Morris, R. T. (1988). "A Weakness in the 4.2 BSD UNIX TCP/IP Software." DOI: 10.6028/NBS.IR-4491
[5]. Neumann, P. G. (1994). "Computer-Related Risks." Chapter 4: "CERT and the Internet." DOI: 10.5555/216585
[6]. Singh, S. (1999). "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography."
[7]. https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/brief-history-of-cybersecurity.html
[8]. Harkins, J., & Bowne, A. (2002). "Planning for Y2K".
[9]. Kaspersky, E. (2012). "Flame: The Story of the Great Cyberweapon".
[10]. Scarf one, K., & Mell, P. (2013). "Guide to Intrusion Detection and Prevention Systems (IDPS)." NIST Special Publication 800-94
[11]. https://www.iso.org/standard/44375.html
[12]. https://www.enisa.europa.eu/topics/definitions-glossary
[13]. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf
[14]. https://ieeexplore.ieee.org/
[15]. https://dl.acm.org/
[16]. https://www.usenix.org/
[17]. https://www.sans.org/reading-room/
[18]. https://www.blackhat.com/
[19]. https://www.defcon.org/
[20]. https://ieeexplore.ieee.org/
[21]. https://ieeexplore.ieee.org/
[22]. https://www.virusbulletin.com/
[23]. https://www.usenix.org/
[24]. https://www.malwaretech.com/2016/10/mirai-a-lurking-threat-that-surprised-the-cybersecurity-industry.html

[25]. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/lifecycle-necurs-botnet/

[26]. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/necurs-the-resilient-botnet-that-just-won-t-quit

[27]. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/zeus-gameover-prolific-banking-trojan-evolves-again

[28]. https://www.europol.europa.eu/newsroom/news/global-avalanche-takedown-operation-disrupts-malware-network

[29]. "Phishing: A Primer of Techniques, Tactics, and Analysis" by Rohyt Belani and Nish Bhalla. In IEEE Security & Privacy, 2007.

[30]. "A Study of Phishing Emails and Tactics: What to Look Out For" by Diana Smetters, et al. In Proceedings of the 2006 Symposium on Usable Privacy and Security (SOUPS), 2006.

[31]. "Password Cracking Attacks and Countermeasures" by Ramakrishnan Durairajan and Charles Kanakan. In the International Journal of Computer Applications, 2011.

[32]. https://www.mcafee.com/enterprise/en-gb/security-awareness/cyber-security/the-advantages-of-cybersecurity.html

[33]. https://www.ibm.com/topics/cybersecurity

[34]. https://www.cisco.com/c/en/us/products/security/security-infrastructure/business-advantage-cybersecurity.html

[35]. https://www.symantec.com/content/dam/symantec/docs/about/annual-report-2020/symantec-2020-corporate-social-responsibility-report.pdf

[36]. https://www.enisa.europa.eu/topics/cs-certification/certification-and-standardisation

[37]. https://www.wipo.int/export/sites/www/sme/en/documents/ip_panorama_15_e_security.pdf

[38]. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

[39]. https://www.iso.org/standard/54534.html

[40]. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

[41]. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

[42]. https://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf

[43]. https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

[44]. https://www.sciencedirect.com/science/article/pii/S1353795308000023

[45]. https://www.ic3.gov/media/2019/191002.aspx

DOI: 10.48175/568