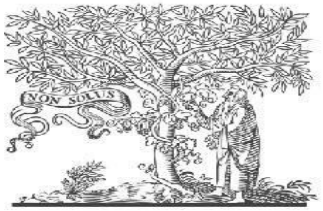
International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

COPY RIGHT



ELSEVIER SSRN

IJIEMR Transactions, online available on 12th Oct 2023. Link :http://www.ijiemr.org/downloads.php?vol=Volume-12&issue=Issue 10

10.48047/IJIEMR/V12/ISSUE 10/11

Title **STUDY ON CYBER SECURITY**

Volume 12, ISSUE 10, Pages: 95-103

Paper Authors **Bhavana Soor, Bhavika Mhasaye, Devendra Dhote, Devesh Pande, Gaurav Thote**

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

STUDY ON CYBER SECURITY

Bhavana Soor[1], Bhavika Mhasaye[2], Devendra Dhote[3], Devesh Pande[4], Gaurav Thote[5]
Student (UG) Department of Computer
Engineering Jagdambha College of Engg. & Tech.
Yavatmal
bhavanasoor@gmail.com,
bhavikamhasaye63@gmail.com,dhotedevendra809@gmail.com
,deveshanandpandeytl@gmail.com,gaurav00379@gmail.com

Abstrct:

In the current world that is run by technology and network connections, it is crucial to know what cyber security is and to be able to use it effectively. Systems, important files, data, and other important virtual things are at risk if there is no security to protect them. Whether it is an IT firm, or every company must be protected equally. With the development of the fresh technology in cyber security, the attackers similarly do not collapse behind. They are consuming better and enhanced hacking techniques and aim the weak points of many businesses out there. Cyber security is essential because the military, government, financial, medical and corporate organizations accumulate, practice, and stock unprecedented quantities of data on PCs and other devices. An important quota of that data can be sensitive information, whether that be financial data, intellectual property, personal information, or other various kinds of data for which illegal access or acquaintance could ensure negative concerns.

Keywords: - Awareness about cyber security, types, benefits.

History :

Cybersecurity has become a familiar subject in both professional and personal lives since the Internet's arrival and the digital transformation initiated in recent years. The Ware Report and the NIST publication introduced the CIA triad of confidentiality, integrity, and availability as key security goals. In the 1970s and 1980s, there were no grave computer threats, as computers and the internet were still developing. More often, threats came from malicious insiders who gained unauthorized access to sensitive documents and files. By the second half of the 1970s, established computer firms like IBM started offering commercial access control systems and computer security software products. The first documented case of cyber espionage occurred between 1986 and 1987, led by Markus Hess. In 1988, the Morris worm gained significant mainstream media attention. Netscape developed the SSL protocol in 1993, but it was never released due to serious security vulnerabilities. The National Security Agency (NSA) protects U.S. information systems and collects foreign intelligence. It analyzes software to identify security flaws for offensive purposes against competitors. Contractors create click-and-shoot attack tools, which are later used by foreign adversaries. In 2016, NSA's hacking tools were hacked by Russia and North Korea. In 2007, the U.S.

and Israel exploited security flaws in Microsoft Windows to attack Iran.

1. Introduction:

Today, anyone may send and receive information via email, video, or other means with the touch of a button, but did they ever consider how secure this information was being sent to the recipient? data?

Cybersecurity is the ideal response. More than 61% of all available capacity is now occupied. Because business exchanges take place online, this sector requires good quality for the best and direct exchanges of security. So, cybersecurity has emerged as one of the most (Dervojeda, et al., 2014) Recent issue. Cybersecurity's scope does not just limit data verification to the IT business, but also to other fields like digital spaces, etc. strengthening cybersecurity and making sure required Data systems are essential to the security of every nation.

Making the Internet more secure (and protecting Internet users) has become to be equally as crucial to the development of new management as a legislative plan. The fight against cybercrime requires a comprehensive and secure approach. (Gross, Canetti, & Vashdi, 2017) Practice. Only the specific estimates may Keep any crime; it's crucial that law enforcement offices are permitted to efficiently investigate and prosecute cybercrime. Currently, several nations and Administrations are mandating strong cyber safety regulations to prevent the loss of a few crucial facts. Each individual should have this cybersecurity equipment and save defending themselves against these rising cybercrimes.

According to Kumar and Somani (2018), cyber-security is both the insecurity created by and through this new environment and the techniques or procedures used to make it (gradually) secure. It alludes to numerous practices and actions, both specialist and non-specialized, that are anticipated to protect the bioelectrical state and the data it holds and transmits from all potential dangers. This study attempts to compile all available data and an overview of cybercrime, as well as historical information and reports on the data analyzed from various attacks that have been widely published over the past five years. We would like to offer all the remedies that organizations may implement to ensure greater security that would aid in protecting the organizations from being attacked based on the information that has been analyzed.

2. Purpose:

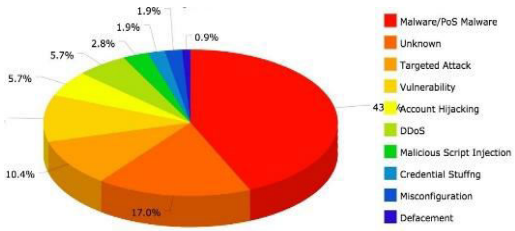
Information regarding cyber security and cybercrime is provided in the paper. terrorism. Its subsections provide a variety of information on these subjects. This defines cybersecurity trends and social media's involvement in cybersecurity. paper. The report offers some important data on cyberterrorism. The both the "cyber terrorism’s constituent parts and its effects Describe in this essay. There are several case study examples that are related to cybersecurity. The document offers several cyber security measures as well. and electronic terrorism. It offers some methods for stopping cyberterrorism. It defines the field of study and application of cybersecurity.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

Over the past ten years, cybersecurity has grown to be a significant problem in the IT industry. Everyone in the modern world struggles greatly with cybercrime. People are extremely concerned as hackers are stealing highly sensitive data from government and some enterprise groups. A cybersecurity attack might result in anything from widespread fraud to the blackmail of major corporations. There are numerous new types of cybercrimes that affect everyone. Be aware of scams and here are the different methods and tools.
can be used to prevent cybercrime. Every organization wants to make sure Their confidential data is resistant to hacking. Being hacked is not just about losing confidential data but losing relationship with customers in the market (Bendovsky, 2015).

The Internet is the fastest growing infrastructure today. In today's technological environment, many new technologies are changing humanity. But because of emerging technology, we cannot protect our personal information in such a way effectively, causing cybercrime to increase rapidly every day. The majority of both commercial and personal transactions are carried out by means of online therefore, it is important to have specialized knowledge that requires a high level of expertise. Security by maintaining better transparency for everyone and having more security transactions. Therefore, network security is the ultimate issue. Technology as advanced as the cloud services, mobile phones, e-commerce, online banking and many more, they claim high standards and safer security processes. All tools and technology participating in these transactions hold the most important and sensitive user's information. Therefore, it is very important to provide them with the necessary security. Improve network security and protect sensitive data and Infrastructure is critical to each country's priority security (Panchanatham, 2015).

3. Types of Cyber Attack



3.1 Malware Attack: Malware is malicious software designed to harm, compromise, or exploit computer systems, networks, and data, posing a significant cybersecurity threat by cybercriminals.
There are various types of malwares, each with distinct characteristics and purposes:

- Viruses: Viruses attach to legitimate files and spread through execution, replicating and spreading across systems.

- Worms: Worms replicate, spread across networks, exploit security vulnerabilities, and exploit operating systems or software.
- Trojans: Trojans are deceptive programs disguised as legitimate software, containing malicious code, posing security risks.

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

- Ransomware: Ransomware encrypts files or systems, causing significant disruption and attracting cybercriminals for lucrative profits.

- Spyware: Spyware steals information from a victim's device, capturing keystrokes, logging activities, and monitoring user behavior.
- Rootkits: Rootkits enable persistent system access by modifying core components, hiding presence and activities, making them difficult to detect.

- Botnets: Botnets are networks of compromised computers controlled by a botmaster, used for coordinated attacks, spam distribution, and malicious activities.

- Keyloggers: Keyloggers record computer keystrokes, enabling attackers to steal sensitive data.

- Logic Bombs: Logic bombs are code snippets triggered by specific conditions, causing malicious actions like file deletions.

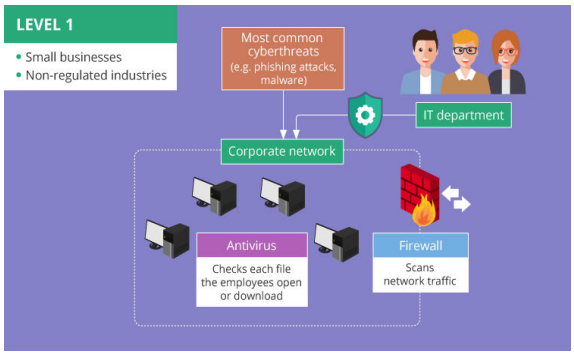
3.2 Phishing Attack: Phishing attacks are cyber attacks that trick individuals into disclosing sensitive information through various communication methods. They disguise themselves as legitimate entities, such as banks or government agencies, to manipulate victims into disclosing sensitive information.

3.3 Man-in-the-Middle (MitM): A Man-in-the-Middle (MitM) attack is a type of cyber-attack that involves an unauthorized actor intercepting and potentially manipulating communications between two parties who believe they are directly communicating with each other. In the context of cybersecurity, MitM attacks pose a significant threat as they can compromise the confidentiality, integrity, and authenticity of sensitive information being exchanged over networks.

3.4 Password Attack: Password attacks are unauthorized attempts to gain access to systems, accounts, or networks by exploiting password weaknesses, targeting sensitive information.

4. Level Of Cyber Security:

Level 1– Minimal protection

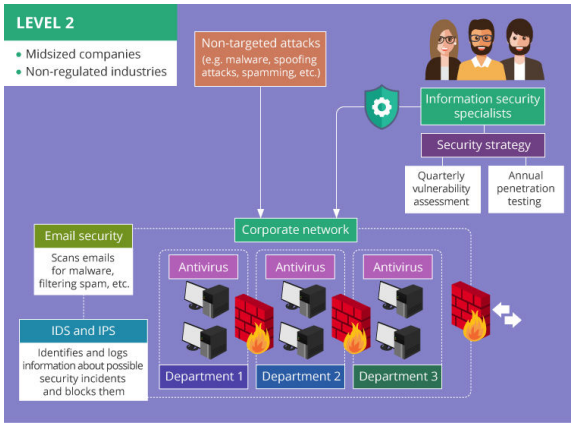


Cybersecurity focuses on protecting a corporate network from common cyberthreats like phishing attacks and malware. This is particularly important for small businesses operating in non-regulated industries with limited financial resources. To implement minimal protection, a properly configured firewall and regularly updated antivirus software are essential. Companies can take responsibility for implementing these measures without a separate cybersecurity department, as firewall protection and antivirus software do not require cybersecurity skills. Regular vulnerability

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

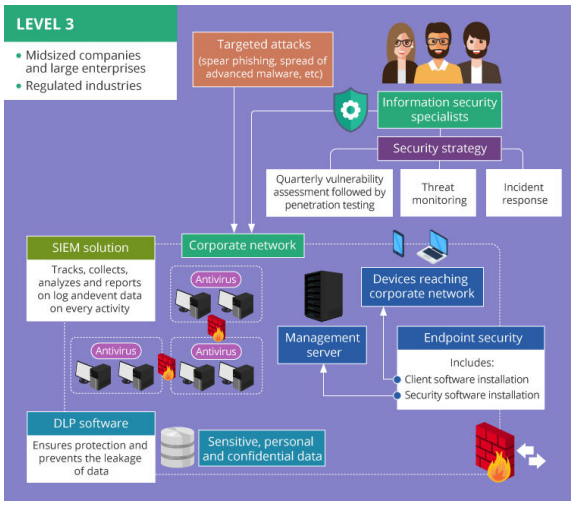
assessment and penetration testing are sufficient for small organizations in non-regulated industries, without requiring significant expenses. These activities help system administrators identify security weaknesses within the company's network.

Level 2 – Advanced protection



Corporate network protection is crucial for midsized companies, as they may be vulnerable to non-targeted attacks. To ensure advanced protection, companies should implement email security, network segmentation, and intrusion detection and prevention systems. Information security specialists are needed to detect and manage cybersecurity risks, develop procedures, and policies. Companies can either establish their own information security department or use managed security service providers (MSSPs). Organizing a separate department can be expensive, but working with an MSSP allows for cost-effective solutions. A cybersecurity strategy should include quarterly vulnerability assessments and annual network penetration testing to detect, mitigate, and manage cybersecurity risks. This strategy should consider staff using personal devices, cloud computing, and provide guidance on acceptable behavior within the corporate network.

Level 3 – Maximal protection



In cybersecurity focuses on protecting a corporate network from targeted attacks, particularly in regulated industries like banking or healthcare. Companies operating in these industries should prioritize protection while adhering to regulations and standards. Key components of cybersecurity include endpoint security, data loss prevention (DLP), and security information and event management (SIEM). Endpoint security involves protecting access to the corporate network from devices, allowing real-time visibility of potential security threats. DLP software ensures protection and prevents the leakage of sensitive data, while SIEM solutions track and analyze log data, ensuring compliance with regulations and incident response. Combining the efforts of a separate information security department with the help of an MSSP can provide the best results. Companies can sign an SLA with a cybersecurity services company and delegate cybersecurity responsibilities to an external MSSP, allowing 24/7 security state monitoring and reporting. Key cybersecurity measures

International Journal for Innovative Engineering and Management Research
PEER REVIEWED OPEN ACCESS INTERNATIONAL JOURNAL
www.ijiemr.org

include developing and maintaining a security strategy, conducting vulnerability assessments, conducting quarterly penetration testing, ensuring constant threat monitoring, and organizing a structured incident response. Threat monitoring is increasingly important due to remote hiring and BYOD policies, which require continuous monitoring of the corporate network and endpoints.

5. Phases Of Cyber Security:

5.1 Prepare: This incident response phase includes preparing for a cybersecurity event. During this phase, you must align your organization's personal information policies and sensitive data protection and cybersecurity goals with the organization's technology infrastructure. During this phase of incident response planning, you need to ensure that all employees have some degree of cybersecurity awareness and basic incident response training to deal with network crisis. Everyone should also be aware of their roles and responsibilities in the event of a cyber event. Identifying important assets and valuables and performing incident response tests are also an integral part of this incident response phase. You can have an external auditor perform a detailed assessment of your organization's breach preparedness, or even perform a one-day quick audit of overall compliance and response to your problem.

5.2 Identify: This phase of incident response planning, as the name suggests, involves determining if you have been breached or any of your systems have been compromised. In the event a breach is actually discovered, under this phase of the NIST Cybersecurity Framework you should focus on answering questions like:
- Who discovered the violation?
- What is the level of violation?
- Will this affect the operation?
- What could be the source of compromise, etc.

It is important to document everything during this phase.

5.3 Contain: This incident response phase includes everything you can do to minimize the damage once you have been the victim of a cyber attack.During this phase of your incident response plan, you need to think about what can be done to limit the impact of the breach. What systems can be taken offline? Is it possible and should be to delete something securely?. What is a short-term strategy?. What is the long-term strategy for dealing with the effects of an attack?. All of these questions need to be answered in phase 3 of the cyber incident response plan. This phase should also include important steps such as reviewing backups, privileged access credentials, and checking that all relevant security updates have been applied.

5.4 Eradicate: Phase 4 of a cyber incident response plan involves understanding the root cause of the breach and addressing it

in real time. Incident response during this phase will involve fixing system vulnerabilities, removing malware, updating older software versions, and more. Essentially, this stage is doing whatever it takes to ensure that any malicious content is removed from your system. However, make sure that this is done without losing valuable data. Nowadays anyone can be attacked. But if you continue to let traces of malware or security issues infiltrate your system, your reputation can be greatly damaged. Your liability may also increase.

5.5 Recover: As the name suggests, this phase of incident response planning involves getting affected systems back to normal after an attack or incident. Of course, this will depend on whether the vulnerabilities in the systems have been closed and how your company will ensure that these systems are no longer compromised. This phase of the network incident response plan is essential as it checks, monitors, and verifies affected systems. Without proper recovery, it will be difficult to avoid another similar incident in the future. As we know, this can be disastrous for the business and the public image of the organization.

5.6 Lessons Learned: We could take the opportunity and say that this is one of the most important stages of an incident response plan. Yes, anyone can and will be a victim of a violation. However, it is how we handle the violation and what we learn from it that makes all the difference. During this phase, it is essential to gather all members of the incident response team and discuss what happened. It's like a flashback to the attack. This phase must be completed no later than 2 weeks after the incident. During this phase, you will return to the document created in Phase 2. You will be able to evaluate what happened, why it happened, and what was done to prevent the situation. But more importantly, at this stage, the company should discuss whether it could do differently. Are there any gaps in the incident response plan? Is there a department or stakeholder that could be more responsive or different? This phase is about learning from the attack to make sure it doesn't happen again and that if it does, the situation is even better managed. To learn more about how you can better prepare your employees for a cyber-attack, check out our NCSC certified cyber incident response and planning course. If you want to test the effectiveness of your network incident response plans, check out our scenario-based network simulation exercises.

6.Future Study and Scope:

This article will help advance the scientific interest in discovering network security, especially to answer questions about your procedures predict important data and future actions for security models. This study set the background to start enforcing rules for all intents, as indicated by Common security issues and feedback for data systems. This document summarizes many procedures that are connected and can be improved in network security service related to predicting the operational legitimacy of methodologies evaluation standards. Finally, focus on limiting, recovering and removing weakness as main model, basic model and react to constant increasingly progressive (Panchanatham, 2015).

In the next 5 years, cybercrime can cause serious damage in computer science. According to the researchers, they estimated Damage was estimated at nearly 6 trillion USD. So there will be a very bright litter for those who work and solve problems related to cybercrime and provide all necessary security measures. Large organizations like CISCO completely related to network technology is one of the main organizations about the millions of opportunities related to cybersecurity because where are future for information technology security. These are great opportunities too in government-related fields and also in the defense sector to protect national security data from cyber attackers.

7. Conclusion:

Cybersecurity involves both insecurities created by and through this new system space and measures or procedures to protect it (gradually). Cyber verification efforts must lead to a definitive need, or else "Information Technology" shall not be feasibly used by the customer. Terrorist of all things coming will win the wars without firing a single shot just by crushing the country. necessary infrastructure if measures are not taken to manage the prevalence of expanded in such a cyber-attack. They can provide an unknown perspective on your life others, whether they live nearby or on the other side of the world.

"Cyber terrorism" can somehow cause death bad consequences, causing serious damage. Although social networks can be used for cybercriminals, these organizations can't stop using social media because it means essential role in the attention of an organization. Cyber terrorism guaranteed many innocent lives and at the same time return many houses to one the state of affairs is sometimes mentally damaging for affected families. Cyber terrorism is still an important issue in today's society. Are not It's just that the war on cyber terrorism is lagging behind, cybercriminals today attacks are becoming more and more violent and confrontational. network security has an interesting resemblance to terrorism. Ensuring information security, data and matching is much more difficult than breaking into the system.

8. References:

1. Dervojeda, K., Verzijl, D., Nagtegaal, F., Lengton, M., & Rouwmaat, E. (2014). Innovative Business Models: Supply chain finance. Netherlands: Business Innovation Observatory; European Union.

2. Howard, M., & Longstaff, T. A. (1998). A common language for computer security incidents. In Proceedings of the 1998 Workshop on New Security Paradigms (pp. 56-66).

3. Masadeh, S.R., Al-Sewadi, H.A. and Al-Husainy, M.A.F. (2023) ‘A message encryption scheme inspired by Sudoku puzzle’, Int. J. Information and Computer Security, Vol. 21, Nos. 3/4, pp.399–413.

4. Schneier, B. (2000). Secrets and lies: Digital security in a networked world. John Wiley & Sons.

5. Kshetri, N., & Voas, J. (2016). Cybercrime and cybersecurity in the global south. Communications of the ACM, 59(1), 78-85.

6. Singapore's Cyber Security Agency (CSA) - Singapore's national agency overseeing cybersecurity strategy and

operations, providing guidance and promoting awareness.

7. Cyberattacks, cyber threats, and attitudes toward cybersecurity policies. Keren L G Snider, Ryan Shandler, Shay Zandani, Daphna Canetti Journal of Cybersecurity, Volume 7, Issue 1,2021,tyab019. https://doi.org/10.1093/cybsec/tyab019

8. K.-K. R. (2011). The cyber threat landscape: Challenges and future research directions. Computers & Security, 30(8), 719–731.

9. De Joode, A. (2011). Effective corporate security and cybercrime. Network Security, 2011(9), 16–18.

10. Institute for Defense Studies and Analyses, India's cyber security Challenge, First Edition, March 2012.

11. R. M. Johri Principal Director (information Systems) Office of CAG of India, ―Cyber Security – Indian Perspective‖

12. "National Cyber Security Policy-2013". Department Of Electronics & Information Technology, Government Of India. 1 July 2013. Retrieved 21 November 2014.

13. y 2014. [11] "Cyber Security Challenges In India Would Increase". Centre Of Excellence For Cyber Security Research And Development In India (CECSRDI). 18 November 2014.

14. Abomhara, M., & Køien, G. M. (2015). Cyber security and the internet of things: Vulnerabilities, threats, intruders and attacks. Journal of Cyber Security, 4(1), 65.