WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

An Examination of Cyber Security: Addressing Challenges and Observing Emerging Trends in Technologies

Mahesh Kumar Tiwari [a], ***Rakchit Seth*** [b], ***Vinayak Tripathi*** [c]

[a] Bachelors of Computer Application, National Post Graduation College, Lucknow, India
[b] Bachelors of Computer Application, National Post Graduation College, Lucknow, India
[c] Bachelors of Computer Application, National Post Graduation College, Lucknow, India
maheshyogi26@gmail.com, rakchitseth@gmail.com, Vinayaktripathimic@gmail.com

ABSTRACT

Cybersecurity holds significant importance within the realm of information technology. Safeguarding information has emerged as a paramount challenge in contemporary times. Whenever cyber security is pondered upon, the foremost thought that arises is the surge of cybercrimes, escalating with each passing day. Governments and corporations are implementing numerous measures to combat these cyber threats. However, despite these efforts, cyber security remains a major concern for many. This paper predominantly delves into the challenges encountered by cyber security in light of recent technologies. It also examines the latest advancements in cyber security techniques, ethical considerations, and the evolving trends shaping the landscape of cyber security.

KEYWORD: Cybersecurity; cybercrime; cyber ethics; social media; cloud computing; android apps

1. Literature Review

1.1 Eight Trends Changing Network Security by James Lyne

In this Sophos article, Lyne highlights eight significant trends that are reshaping network security. The trends encompass various aspects such as emerging technologies, evolving cyber threats, and changing strategies for defense. Lyne's insights provide valuable perspectives for understanding the contemporary challenges and opportunities in network security.

1.2 Cyber Security: Understanding Cyber Crimes by Sunit Belapure et.al

Belapure and Godbole delve into the intricate landscape of cybercrimes, offering comprehensive insights into their nature, motivations, and impact on individuals, organizations, and society at large. Their work aids in enhancing understanding and awareness regarding the multifaceted dimensions of cyber security threats.

1.3 Computer Security Practices in Non-Profit Organizations by Audrie Krause

Krause's Net Action report sheds light on the specific challenges and practices related to computer security in non-profit organizations. By examining the unique needs and constraints faced by these entities, Krause provides valuable guidance for improving security posture in this sector.

1.4 A Look Back on Cyber Security 2012 by Luis Corrons

Corrons' retrospective analysis offers a detailed examination of key events, trends, and developments in cyber security during the year 2012. By revisiting past experiences and lessons learned, Corrons provides valuable insights for understanding the evolution of cyber threats and defenses over time.

1.5 Study of Cloud Computing in Healthcare Industry by G. Nikhita Reddy et.al

Reddy and Reddy's research investigates the adoption and implications of cloud computing in the

healthcare sector. By examining the intersection of cloud technology and healthcare operations, their study contributes to understanding the unique cyber security challenges and opportunities within this critical industry.

Safety Critical Systems - Next Generation in IEEE Security and Privacy Magazine

This IEEECS article explores the evolving landscape of safety critical systems, focusing on emerging technologies and methodologies. By addressing the intersection of safety and security concerns in next- generation systems, the article provides valuable insights for ensuring the resilience and reliability of critical infrastructures.

1.6 Cyber Security in Malaysia by Avanthi Kumar

Kumar's analysis of cyber security in Malaysia offers a localized perspective on the challenges and initiatives in combating cyber threats within the country. By examining the socio-political, economic, and technological factors at play, Kumar's work contributes to a deeper understanding of cyber security dynamics in the Malaysian context.

2. Introduction

In the present era, individuals can effortlessly transmit various forms of data, such as emails, audio, or video, with a simple click. However, amidst this convenience, it's crucial to consider the security of data transmission to ensure confidentiality and integrity. This underscores the significance of cyber security. The internet stands as the rapidly expanding backbone of modern daily life, facilitating numerous technological advancements that shape human existence. However, the emergence of these technologies has presented challenges in safeguarding private information effectively, leading to a surge in cybercrimes.

With over 60 percent of commercial transactions now conducted online, the need for robust security measures to facilitate transparent and secure transactions is paramount. Consequently, cyber security has emerged as a pressing concern. Its scope extends beyond the confines of the IT industry, encompassing various domains such as cyberspace. Even cutting-edge technologies like cloud computing, mobile computing, e-commerce, and online banking demand high-level security due to the sensitive nature of the information they handle.

Enhancing cyber security and safeguarding critical information infrastructure are crucial for national security and economic stability. As the internet plays an increasingly integral role in the development of new services and governmental policies, ensuring its safety and protecting users' interests has become imperative. Combatting cyber-crime necessitates a multifaceted approach that goes beyond technical measures alone. Effective investigation and prosecution by law enforcement agencies are essential in this endeavor.

To address the growing threat of cyber-crimes, many nations and governments have implemented stringent laws pertaining to cyber security to mitigate the risk of data breaches. Moreover, individuals must also be equipped with adequate knowledge and training in cyber security to protect themselves from potential threats in this digital landscape.

3. Cyber Crime

Cyber-crime encompasses any unlawful activity carried out primarily through the use of a computer. The U.S. Department of Justice broadens this definition to include any illicit activity utilizing a computer for evidence storage. The spectrum of cyber-crimes continues to expand, encompassing offenses facilitated by computers, such as network intrusions and the distribution of computer viruses, alongside computer- enabled iterations of traditional crimes like identity theft, harassment, bullying, and terrorism. These offenses pose significant challenges to individuals and nations alike.

In simpler terms, cyber-crime refers to criminal acts committed using computers and the internet, ranging from identity theft to the sale of illegal goods, online harassment, and the deployment of malicious software to disrupt operations. As technology increasingly pervades daily life, cyber-crimes are expected to rise in tandem with technological advancements.

3.1 Cyber Security

Ensuring the privacy and security of data remains a paramount concern for any organization. In today's digital age, where information is predominantly stored in cyber formats, maintaining robust security measures is imperative. While social networking platforms offer a sense of security for users to engage with friends and family, they also become prime targets for cyber-criminals seeking to pilfer personal data. Similarly, individuals must exercise caution during online banking transactions, implementing necessary security protocols.

According to a survey conducted by Silicon Valley Bank among technology and healthcare executives nationwide, the threat of cyber-attacks is perceived as a significant risk to both data integrity and business continuity. The findings reveal that 98% of companies are either maintaining or increasing their cybersecurity resources, with half of them allocating additional resources specifically to combat online attacks. Despite these efforts, the majority of companies acknowledge the inevitability of cyber-attacks and are actively preparing for such occurrences. However, confidence in the security of information remains low, with only one-third expressing complete assurance, particularly concerning the security measures implemented by their business partners.

Predictions in cyber security indicate the likelihood of new attacks targeting Android-based devices, albeit not on a massive scale. As tablets share the same operating system as smartphones, they are susceptible to similar malware threats. Additionally, the proliferation of malware specimens for Macs is

anticipated to continue, albeit at a slower pace compared to PCs. With Windows 8 enabling the development of applications for various devices, including PCs, tablets, and smartphones, there's a growing concern about the potential emergence of malicious applications similar to those targeting Android devices. These trends underscore the evolving landscape of cyber security and the ongoing need for vigilance and proactive measures to mitigate risks.

Incidents	Jan- June 2012	Jan- June 2013	% Increase/ (decrease)
Fraud	2439	2490	2
Intrusion	2203	1726	(22)
Spam	291	614	111
Maliciouscode	353	442	25
Cyber Harassment	173	233	35
Contentrelated	10	42	320
IntrusionAttempts	55	24	(56)
Denial ofservices	12	10	(17)
Vulnerabilityreports	45	11	(76)
Total	5581	5592	

Table 1

The comparison of cyber security incidents reported to Cyber999 in Malaysia for the periods of January to June 2012 and 2013 vividly illustrates the prevailing cyber security threats. As criminal activities escalate, security measures are correspondingly heightened. This trend is echoed in a survey conducted in the United States.

4. Evolving Patterns Cyber Security

Below are some trends that significantly impact cyber security:

4.1 Web Servers:

The persistent threat of attacks on web applications aimed at extracting data or distributing malicious code remains prevalent. Cybercriminals leverage compromised legitimate web servers to distribute their malicious code. Data-stealing attacks, which often garner media attention, pose a significant threat as well. It is imperative to prioritize the protection of web servers and web applications. Web servers serve as prime targets for cybercriminals seeking to steal data. Therefore, it is essential to use secure browsers, particularly during critical transactions, to mitigate the risk of falling victim to such crimes.

4.2 Cloud Computing and Its Offerings:

Companies of all sizes are increasingly adopting cloud services, marking a notable shift towards cloud computing. This trend poses a substantial challenge for cyber security as traffic can circumvent traditional inspection points. Additionally, as the repertoire of applications available in the cloud expands, policy controls for web applications and cloud services must evolve to prevent data loss. Despite the evolving security models of cloud services, concerns about their security persist. While the cloud presents vast opportunities, it is essential to recognize that as the cloud evolves, so do its security challenges.

4.3 Advanced Persistent Threats (APTs) and Targeted Attacks

Advanced Persistent Threats (APTs) represent a sophisticated form of cybercrime. Traditional network security capabilities, such as web filtering or Intrusion Prevention Systems (IPS), have historically played a crucial role in identifying targeted attacks, often after the initial compromise. As attackers employ increasingly obscure techniques, network security must integrate with other security services to detect such attacks. Enhancing security techniques is essential to thwarting future threats posed by APTs and targeted attacks.

4.4 Mobile Networks:

The widespread connectivity facilitated by mobile networks raises significant security concerns. Firewalls and other security measures are becoming increasingly porous as individuals utilize various devices, including tablets, phones, and PCs, each requiring additional security measures beyond those present in the applications used. The security issues surrounding mobile networks must be carefully considered and addressed to mitigate cybercrime risks effectively.

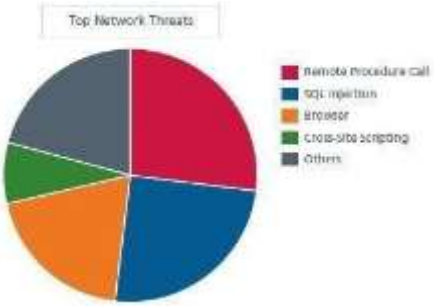
4.5 IPv6: New Internet Protocol:

IPv6, the new Internet protocol replacing IPv4, which has long served as a backbone of networks and the Internet, introduces significant changes to network infrastructure. Protecting IPv6 requires more than simply porting IPv4 capabilities. While IPv6 expands the availability of IP addresses, fundamental protocol changes necessitate careful consideration in security policy formulation. Thus, transitioning to IPv6 is advisable to reduce cybercrime risks effectively.

4.6 Encryption of Code:

Encryption involves encoding messages or information in a manner that prevents eavesdroppers or hackers from deciphering it. This process entails using encryption algorithms to transform information into unreadable ciphertext, often with the aid of encryption keys. While encryption safeguards data privacy and integrity, increased usage presents challenges in cyber security. Encryption is crucial for protecting data in transit, such as data transferred via networks or mobile devices. Encrypting code aids in detecting information leaks and enhances overall data security.

Hence the above are some of the trends changing the face of cyber security in the world.The top network threats are mentioned in below



The above pie chart shows about the major threats for networks and cyber security

5. Role of Social Media in Cyber Security

As our interactions become increasingly social in a digitally interconnected world, companies are faced with the challenge of safeguarding personal information. Social media platforms significantly influence cyber security and pose considerable threats to personal data. The widespread adoption of social media among individuals has led to a surge in potential attacks. Given the ubiquity of social networking sites in daily life, they have become prime targets for cybercriminals seeking to exploit private information and pilfer valuable data.

In a society where the disclosure of personal information is commonplace, companies must swiftly identify and address threats in real time to prevent breaches. Cybercriminals capitalize on people's inclination towards social media, using it as a lure to obtain sensitive information. Therefore, individuals must adopt appropriate measures, particularly when engaging with social media, to mitigate the risk of data loss.

The capacity for individuals to share information with vast audiences underscores the unique challenge that social media poses for businesses. Apart from enabling the dissemination of commercially sensitive information, social media also facilitates the rapid spread of false information, which can be equally detrimental. The Global Risks 2013 report identifies the swift propagation of false information through social media as one of the emerging risks.

Despite the potential for social media to be exploited for cybercrimes, companies cannot afford to disengage from these platforms, given their critical role in publicity. Instead, they must implement solutions capable of detecting threats and mitigating them before substantial damage occurs. Companies should acknowledge the necessity of analyzing information, particularly within social conversations, and provide tailored security solutions to mitigate risks. Utilizing specific policies and appropriate technologies is crucial for managing social media effectively.

6. Cyber Security Techniques

6.1 Access Control and Password Security

The traditional method of using usernames and passwords has long been a cornerstone of information protection and is often regarded as one of the initial steps in cyber security.

6.2 Data Authentication

Prior to downloading documents, it is imperative to ensure their authenticity, verifying that they originate from trusted and reliable sources and remain unaltered. Typically, document authentication is carried out by antivirus software installed on devices, underscoring the importance of robust antivirus protection.

6.3 Malware Scanners

Malware scanners are software tools designed to scan all files and documents within a system for malicious code or harmful viruses. Malicious software, such as viruses, worms, and Trojan horses, collectively referred to as malware, are detected and identified by these scanners.

6.4 Firewalls

Firewalls, whether in the form of software programs or hardware devices, serve as a crucial line of defense against hackers, viruses, and worms attempting to infiltrate computers via the Internet. By scrutinizing all incoming and outgoing messages, firewalls assess each message against predetermined security criteria and block those that fail to meet the specified standards, thus playing a pivotal role in malware detection.

6.5 Antivirus Software

Antivirus software constitutes a vital component of cyber security, capable of detecting, preventing, and neutralizing malicious software programs, including viruses and worms. Most antivirus programs feature an auto-update functionality, allowing them to download new virus profiles promptly and thereby promptly identify and address emerging threats. Thus, antivirus software stands as an essential and foundational requirement for every system's security.

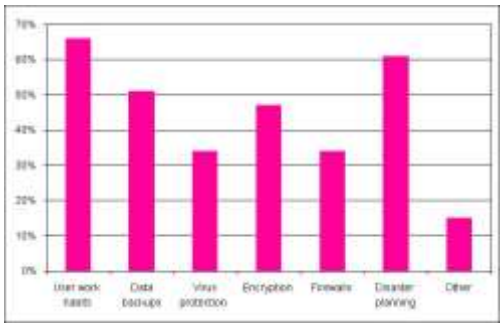


Table 2: **Techniques on cyber security**

7. Cyber Ethics

Cyber ethics represent the guiding principles governing behavior on the internet. Adhering to these principles enhances our utilization of the internet in a responsible and safer manner. Here are some key cyber ethics to observe:

- Utilize the internet for communication and interaction with others, leveraging tools like email and instant messaging to connect with friends, family, and colleagues, as well as share ideas and information globally.
- Refrain from engaging in cyberbullying activities, such as name-calling, spreading lies, or sharing embarrassing content about others.
- Recognize the internet as a vast repository of knowledge and information, and use it in a lawful and appropriate manner.
- Avoid accessing others' accounts using their passwords, respecting their privacy and security.
- Refrain from distributing malware or attempting to compromise others' systems.
- Safeguard personal information and refrain from sharing it with unauthorized individuals to prevent potential misuse and subsequent trouble.
- Maintain authenticity online, refraining from impersonating others or creating fake accounts, which could lead to legal consequences for both parties involved.
- Respect copyright laws and obtain permission before downloading or sharing copyrighted materials, such as games or videos.

Adherence to these cyber ethics is essential for responsible internet usage. Just as we are taught proper conduct from an early age, applying similar principles in cyberspace ensures a safer and more ethical online environment.

8. Conclusion

Computer security is an expansive subject matter that is gaining increasing importance as the world becomes more interconnected, relying on networks for vital transactions. With each passing year, cybercrime takes on new dimensions, evolving alongside the security measures put in place to protect information. The emergence of disruptive technologies, coupled with the daily unveiling of new cyber tools and threats, presents organizations with

significant challenges in securing their infrastructure. Addressing these challenges necessitates the adoption of new platforms and intelligence. While there is no foolproof solution to cybercrimes, it is imperative to exert maximum effort in minimizing their occurrence to ensure a safe and secure future in cyberspace.

References

1. A Sophos Article 04. 12v1.dNA, eight trends changing network security by James Lyne
2. Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole
3. Computer Security Practices in Non-Profit Organisations – A Net Action Report by Audrie Krause.
4. A Look back on Cyber Security 2012 by Luis corrons – Panda Labs.
5. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page nos.68 – 71 ISSN 2229-5518, Study of Cloud Computing in HealthCare Industry by G. Nikhita Reddy, G.J. Ugander Reddy
6. IEEE Security and Privacy Magazine – IEEECS Safety Critical Systems – Next Generation July/ Aug 2013.
7. CIO Asia, September 3rd, H1 2013: Cyber security in Malasia by Avanthi Kumar