***DOI:** https://doij.org/10.10000/IJLMH.1110269*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 3

2025

Cyber Nexus: Forging Tomorrow's Laws for Today's Threats

VAIBHAV SALUNKHE[1] AND VINAYAK MODANWAL[2]

ABSTRACT

This research paper aims to be aware and educate about emerging cyber security threats and challenges. Cyber security challenges have been prevalent nowadays, and new and effective solutions must be implemented to reduce these negative impacts. Cyber security is required in every organisation to protect every specific data category from damage and theft. It mainly includes personally identifiable information, intellectual property, data, organisational information systems and many more. Hence, the organisational data and information would be safe and secured under every circumstance, and the data management aspects would be enhanced to a high level. This research paper has considered a literature review of recent articles on cyber security challenges and emerging trends in cloud computing. Six cyber security risks are identified, and three emerging cloud trends are determined from the existing research. This research paper also provides future research avenues that would benefit the technological aspect. Cybersecurity threats are rapidly evolving, posing significant challenges to individuals, organizations, and governments worldwide. This research paper examines emerging cyber security threats and explores the development of futuristic techno-legal standards and frameworks to enhance conviction rates in cyber-crimes. By analyzing current trends, potential future risks, and the intersection of technology and law, this study proposes proactive measures to combat cyber threats effectively. This paper explores the emerging challenges posed by these threats and the limitations of current techno-legal frameworks in addressing them. It proposes the development of futuristic techno-legal standards that leverage technological advancements and legal reforms to improve cyber crime investigation, prosecution, and ultimately, conviction rates.

I. INTRODUCTION

Cyber security is an important issue in the infrastructure of every company and organization. Cyber security refers to the core practice to protect various systems, networks, and different programs from digital attacks. Stealing attacks against controlled information, along with the increasing number of information leakage incidents, has become an emerging cyber security

[1] Author is an Advocate in India.

[2] Author is a Student at Bharati Vidyapeeth New Law College, Pune, India.

threat in recent years. All of such cyber-attacks are mainly aimed at accessing, destroying and changing personal information or even interrupting normal business processes. Hence, the user is able to secure their system from unauthorized exploitation of systems, technologies and networks .Proper implementation of the most effective measures of cyber security is extremely challenging as there are several devices than various individuals, and the attackers are becoming highly innovative. In spite of such advantages, there are a few prevalent challenges in cyber security that are needed to be eradicated for gaining maximum efficiency. The following research paper outlines a brief discussion on cyber security challenges and different emerging trends in cloud computing.

II. Cyber world: a soma or curse

Today man is able to send and receive any form of data, be it an e-mail or an audio or video just by the click of a button but did he ever think how securely his data ID being transmitted or sent to the other person safely without any leakage of information?? The answer lies in cyber security. Today the Internet is the fastest growing infrastructure in everyday life. In Today's technical environment many latest technologies are changing the face of mankind. But due to these emerging technologies we are unable to safeguard our private information in a very effective way and hence these days cyber crimes are increasing day by day.

Today more than 60 percent of total commercial transactions are done online, so this field requires a high quality of security for transparent and best transactions. Hence cybersecurity has become the latest issue. The scope of cyber security is not just limited to securing the information in the IT industry but also to various other fields like cyber space etc.Even the latest technologies like cloud computing, mobile computing, E-commerce, netbanking etc also needs a high level of security.

Since these technologies hold some important information regarding a person their security has become a must thing. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic wellbeing. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as governmental policy. The fight against cyber crime needs a comprehensive and a safer approach. Given that technical measures alone cannot prevent any crime, it is critical that law enforcement agencies are allowed to investigate and prosecute cyber crime effectively.

Today many nations and governments are imposing strict laws on cyber securities in order to prevent the loss of some important information. Everyindividual must also be trained on this cybersecurity and save themselves from these increasing cyber crimes.

III. EMERGING CYBER SECURITY THREATS AND CHALLENGES

The total dependency of the world on the Internet for even the most basic things has made data security the need of the hour. Now, if we look at the amount of sensitive information the Internet carries, from your home address to your credit card details, cybersecurity challenges become indispensable. According to CheckPoint Research, global cyberattacks increased by 38% in 2022, compared to 2021. This increase was driven by a number of factors, including the rise of remote work, the increasing use of cloud computing, and the growing sophistication of cybercriminals.

Likewise, in 2022, data breaches dominated the headlines. Companies from Twitter to Microsoft to American Airlines were the victims of data breaches as cybercriminals continued to wreak havoc in enterprises, disrupting business continuity and hindering business success. Data breaches like these impacted 422.1 million people last year, a 41.5% increase over 2021, according to the Identity Theft Resource Center (ITRC).

LoT Attacks (Internet of Things)

The Internet of Things or IoT is the most vulnerable to data security threats. Every digital, mechanical, computing smart device that can transmit data over the internet network are termed as IoT such as; laptop and mobile phones.In order to access your personal device that contains your sensitive information, hackers use devices that surround you, such as wearable smartwatches, baby monitors, smart fridges, or smart lights.The IoT sector is the primary target for hackers looking to access users’ sensitive data. In 2024, the number of connected devices is predicted to increase to more than 14.4 billion. IoT Analytics claims that by 2025, there will be more than 27 billion gadgets online simultaneously. Around 12 billion devices were online by 2022, and this figure will rise to 25 billion by the end of 2030, as per the data.As a result it will open a wide space for the hackers to attack the compromised data security and use them for malicious purposes.

Cloud Attacks

Cloud computing is the modern era of new technology that revolutionized the physical world of data storage. Businesses from large to small now utilize cloud services for storing their user-sensitive information. On the one hand, where adoption of it has reduced the cost and increased efficiency, it has also opened possibilities for data security breaches.

The main reason for compromised data security is the lack of encryption, authentication, and improper configuration of the cloud setups. So, they need to maintain many considerations for cloud security and data protection, to keep the sensitive information intact.A recent case of Microsoft 2021 had made headlines, where the enterprise suffered a denial of service attack that made it almost impossible to access their cloud data service.

In their official statement, Microsoft stated that the attack lasted for 10 mins and they were able to dodge the attack. "Business as usual for Azure customers despite 2.4 TBPS DDoS attack" Still, it gives a fact check on how even the leading companies like Microsoft that practices strict cybersecurity protocols face cloud attack. In light of this, even small firms and professionals who use cloud setups are not-at-all exempted from these attacks.

Phishing Attacks

A phishing attack is a type of social engineering attack that targets users' login details and credit card information. In contrast to ransomware, here the information benefits the hacker. Gmail is a Google service that is used across the board for almost everything from business to personal purposes.

Now, whenever you open your mail account, you might come across a spam folder that consists of emails that the platform recognizes as a threat to your data security. These spam emails consist of thousands of phishing attacks that your mailing partner recognizes and warns you about the potential cyber threat that it carries. Yet, some of the communications still make it to your inbox where you might fall into a trap.

Officially, Google released a statement of how it blocks more than 100 million phishing emails on an everyday basis. It further emphasized how most of the communications were trying to impersonate government officials, authorities, agencies, or websites in order to sound more reliable to mail recipients.

Ransomware Attacks

Ransomware is one of the biggest cyber security challenges that concerns us in the digital world. In the year 2021- 2022, there were an unparalleled number of ransomware attacks, and this trend is still to continue in 2024.As the word ransom suggests, it's hacking into the user's sensitive information and denying them access to it until a ransom amount is reimbursed to the hackers. Now, businesses that need access to their data to run their daily operations suffer a lot from this breach, highlighting a serious emphasis that needs to be given by them on their data security strategies. As per a study from ASTRA IT, 1.7 million ransomware attacks occur every day, with a ransomware attack occurring every 2 seconds. As much as $1.85 million was lost in the average ransomware assault. The WannaCry ransomware outbreak cost the

National Health Service (NHS) an estimated $100 million.

Besides this, more and more attacks were reported after the pandemic since every information circulated was using the means of digitalization."Still, ransomware attacks are not new. Businesses, governments, and even individuals have been victims of ransomware attacks for over three decades now" – as explained in the detailed article of What is Ransomware? By Sagenext. According to the Financial Trend Analysis report by Fincen (Financial Crime Enforcement Network), suspicious activity related to ransomware SARs in the first half of 2021 estimated $590 million exceeded the total reported for all of 2020 ($416 million).

Insider Attacks

While many cyber threats originate externally, insider attacks—where employees or trusted individuals intentionally or unintentionally compromise sensitive data—are a growing concern. According to a 2024 report, 83% of organizations experienced at least one insider attack in the past year, a sharp increase linked to the complexity of hybrid work environments and widespread cloud adoption. Such breaches can severely damage a company's finances and reputation. To mitigate these risks, organizations are increasingly monitoring network traffic, implementing access controls based on job roles, and using centralized security tools to detect suspicious activity.

Social Engineering Attacks

Social engineering remains a major threat, exploiting human psychology to extract confidential information. Attackers use tactics such as phishing emails, voice manipulation, and impersonation to trick employees into revealing sensitive data. In 2024, the average cost of a social engineering attack reached $130,000, and organizations face over 700 such attacks annually. Notably, 68% of data breaches this year involved human error, often facilitated by social engineering. These attacks can lead to significant financial losses and data compromise, highlighting the need for ongoing employee awareness and training.

Man-in-the-Middle (MitM) Attacks

MitM attacks involve cybercriminals intercepting communications between two parties, often exploiting insecure public Wi-Fi or compromised devices. The rise of remote and hybrid work, along with increased use of IoT devices, has made organizations more vulnerable. Attackers can hijack sessions, strip SSL encryption, or eavesdrop on Wi-Fi traffic, leading to unauthorized access to sensitive business information. High-profile incidents in 2024, including telecom hacks and browser extension compromises, have demonstrated the disruptive potential of MitM attacks and the importance of robust encryption and secure network protocols.

Cryptocurrency and Blockchain Attacks

The rapid growth of digital currencies and blockchain platforms has attracted cybercriminals. In 2024 alone, over $2.2 billion was stolen from crypto platforms worldwide. Attackers employ methods such as ransomware, phishing, and exploiting vulnerabilities in wallets and exchanges. Major incidents have forced some platforms to shut down, and the use of complex laundering techniques has made recovery difficult. As blockchain adoption increases, so does the urgency for enhanced security measures to protect investors and digital assets.

Mobile Banking Malware

Cybercriminals are increasingly targeting smartphones and tablets to access banking information. In 2024, there was a 258% surge in mobile banking malware attacks, with nearly 250,000 users affected globally. Malware such as banking Trojans can steal login credentials, credit card information, and other sensitive data, sometimes draining accounts within minutes. The growing sophistication of these attacks underscores the need for strong mobile security and user vigilance.

AI-Driven Attacks

Artificial intelligence is now a double-edged sword in cybersecurity. While AI helps security teams detect and respond to threats, attackers are leveraging AI to automate attacks, create more convincing phishing campaigns, and bypass traditional defenses. In the past year, 87% of global organizations faced AI-powered cyber attacks. AI is also being used to generate malware, adapt ransomware, and create realistic deepfakes for social engineering. As AI technology advances, both the scale and complexity of cyber threats are expected to rise.

IV. Winning war with the cybersecurity challenges of 2024

More than 74% of breaches involve the human element, and the advancement of AI is bringing even more convincing attempts to trick employees. Sophisticated phishing attacks, automated hacking tools, AI-powered social engineering techniques and deepfake threats mean security awareness training and a culture of awareness are more critical for organizations than ever.

The good news is that organizations can shift that human risk and have their employees contribute to a cyber secure environment — with the right training. Practical and engaging security awareness training for employees can provide staff with the knowledge to identify and defend against cyber threats.

As the world of work evolves and AI technology grows, so are security threats. When designing your best security awareness training program, covering the cyber threats your organization will most likely face is essential. These are the 10 most important security awareness topics to include in security awareness training for employees.

Email scams

Phishing attacks are the most common method that cybercriminals use to gain access to an organization's network. So it's no surprise that they lead our security awareness topics list.

They take advantage of human nature to trick their target into falling for the scam by offering some incentive (free stuff, a business opportunity and so on) or creating a sense of urgency. And with AI, fraudsters can quickly refine their messaging to make the most enticing phishing email possible.

Phishing awareness should be a component of any organization's security awareness training. This should include examples of common and relevant phishing emails, such as emails that mimic shipping notifications, tax-related phishing scams, bank alerts and internal corporate communications.

Tips for identifying and avoiding phishing emails include:

- Do not trust unsolicited emails
- Be wary of any email that creates a sense of urgency, secrecy and authority (e.g., leadership asking to send a large payment by the end of the day and to keep it secret as it's not yet public).
- Confirm requests for sensitive data or funds via another medium (such as phone or in person) before responding.
- Be wary of unsolicited email attachments. Verify any unsolicited attachments with the alleged sender via another medium before opening them.
- Remember that these types of attacks can occur across any communication platform (including email, text messages, messaging apps, enterprise collaboration platforms and so on)

In addition, ensure your organization is filtering spam, has its email client and firewall configured correctly, and uses up-to-date antivirus.

Malware

Malware is malicious software that cybercriminals use to steal sensitive data (user credentials, financial information and so on) or cause damage to an organization's systems (e.g., ransomware and wiper malware). Organizations can become infected with malware in several ways, including phishing emails, drive-by downloads (e.g., visiting a malicious site with an out-of-date browser that gets exploited), exploiting application vulnerabilities and malicious removable media.

Employee security awareness training on malware should cover common delivery methods, threats and impacts to the organization. Important tips include:

- Be suspicious of files you download in emails, websites and other mediums
- Don't install unauthorized software
- Keep antivirus running and up to date
- Contact IT/security team immediately if you may have a malware infection

Password security

Passwords are the most common and easiest-to-use authentication system in existence. Most employees have dozens of online accounts accessible via a username (often their email address) and a password.

Poor password security is one of the biggest threats to modern enterprise security. And a solid password security protocol is a crucial security awareness topic. Some important password security tips to include in training content:

- Always use a unique password for each online account
- Follow company password practices, such as long passphrases or randomly generated characters
- Use a password manager to generate and store strong passwords for each account
- Use multi-factor authentication (MFA) when available to reduce the impact of a compromised password

Removable Media

Removable media (such as USBs or external hard drives) are a useful tool for cybercriminals since they enable malware to bypass an organization's network-based security defenses. Malware can be installed on the media and configured to execute automatically with Autorun — or have an enticing filename to trick employees into clicking. Malicious removable media can steal data, install ransomware or even destroy the computer when connected.

A popular example is dropping a USB stick in a parking lot and common areas (bonus for including an enticing label like “Employee compensation”) or handing them out at conferences and other public events. Employees should be trained to properly manage untrusted removable media:

- Never plug untrusted removable media into a computer
- Bring all untrusted removable media to IT/security for scanning
- Disable autorun on all computers

In addition, some organizations may not allow employees to connect any removable media to company machines.

Safe Internet Habits

For most organizations, nearly every employee has access to the internet — and more teams becoming remote has led to a surge in online collaboration. For this reason, building secure online habits across employees is paramount for companies.

Security awareness training for employees should incorporate safe internet habits that prevent attackers from penetrating your corporate network. Some important content to include in training:

- The ability to recognize suspicious and spoofed domains (like yahooo.com instead of yahoo.com)
- The differences between HTTP and HTTPS and how to identify an insecure connection
- The dangers of downloading untrusted or suspicious software off the internet
- The risks of entering credentials or login information into untrusted or risky websites (including spoofed and phishing pages)
- Watering hole attacks, drive-by downloads and other threats of browsing suspicious sites

Social Networking Dangers

Social networking is a powerful tool for enterprises to build brand awareness and generate sales, and each of your employees likely belongs to multiple social networking sites. Unfortunately, cybercriminals use social media in various ways to potentially damage your organization or gain unauthorized access — from harvesting data for a future social engineering campaign to phishing attacks that steal credentials to sharing malicious links that could lead to incidents like ransomware.

To prevent the loss of critical data, your enterprise must have a viable social networking training program that should limit the use of social networking and inform employees of the threats of social media:

- Phishing attacks can occur on social media as well as over email
- Cybercriminals impersonating trusted brands can steal data or push malware
- Social engineers are exceedingly good at taking small pieces of information published on social media to craft convincing spear phishing emails

Physical security and environmental controls

Security awareness isn't just about what resides in your company's computers or handheld devices. Employees should be aware of potential security risks in the physical aspects of the workplace.

Examples of physical security topics include:

- Visitors or new hires watching as employees type in passwords (known as "shoulder surfing")
- Letting in visitors claiming to be inspectors, exterminators or other uncommon guests who might be looking to get into the system (called "impersonation")
- Allowing someone to follow you through a door into a restricted area (called "tailgating")
- Leaving passwords on pieces of paper on one's desk
- Leaving one's computer on and not password-protected when leaving work for the night
- Leaving an office-issued phone or device out in plain sight
- Physical security controls (doors, locks and so on) malfunctioning

Clean desk policy

A clean desk policy is a sometimes-overlooked security awareness topic that ties back to physical security. Sensitive information on a desk, such as sticky notes, papers and printouts, can easily be taken by thieving hands and seen by prying eyes.

A clean desk policy should state that information visible on a desk should be limited to what is currently necessary. Before leaving the workspace for any reason, employees should securely store all sensitive and confidential information

Data management and privacy

Most organizations collect, store and process a great deal of sensitive information. This includes customer data, employee records, business strategies and other data important to the proper operation of the business. Suppose this data is publicly exposed or accessible to a competitor or cybercriminal. In that case, your organization may face significant regulatory penalties, damage to consumer relationships and a loss of competitive advantage.

Employees within an organization need to be trained on how to properly manage the businesses' sensitive data to protect data security and customer privacy. Important training content includes:

- The business's data classification strategy and how to identify and protect data at each level
- Regulatory requirements that could impact an employee's day-to-day operations
- Approved storage locations for sensitive data on the enterprise network
- The use of a strong password and MFA for accounts with access to sensitive data

Bring-your-own-device (BYOD) policy

BYOD policies enable employees to use their personal devices in the workplace. While this can improve efficiency by enabling employees to use the devices that they are most comfortable with, it also creates potential security risks.

Security awareness training for employees should include the following:

- Secure workplace devices with a strong password to protect against theft
- Use a VPN on devices when working from untrusted Wi-Fi
- Follow company policies around additional protection, such as a company-approved antivirus
- Only download applications from major app stores or directly from the manufacturer's website

In addition, the organization may require that full-disk encryption is enabled for BYOD devices and use tools to restrict what can be accessed or shared on the company portion of the device.

Here cyber security challenges of 2024 are complex and ever-changing some of them are:

- Have a strong security posture. This includes having up-to-date security software, strong passwords, and a layered security approach.
- Be aware of the latest threats. Cybercriminals are constantly developing new ways to attack, so it's important to stay up-to-date on the latest threats.
- Educate your employees. Employees are often the weakest link in the security chain. Make sure they are aware of the latest threats and how to protect themselves.
- Have a plan in place. If you get attacked, it's important to have a plan in place to respond quickly and effectively.
- Use a password manager. A password manager can help you create and store strong, unique passwords for all of your online accounts.
- Be careful what you click on. Phishing emails and malicious websites are a common way for cybercriminals to gain access to your systems. Be careful what links you click on and what attachments you open.
- Keep your software up to date. Software updates often include security patches that can help protect you from known vulnerabilities.
- Use a firewall. A firewall can help protect your computer from unauthorized access.
- Back up your data regularly. If your computer is infected with malware or your data is stolen, having a backup can help you recover your data.

V. Conclusion

Therefore, from the above discussion, a conclusion can be drawn that cyber security challenges must be avoided on a priority basis for gaining maximum advantages in the respective organisation. This research paper has identified certain distinct cyber security challenges by conducting a literature review and analysing these threats. The emerging trends of cloud computing also need to be highlighted to gain an idea of better results and efficiency. The research question of cyber security challenges is identified in the paper, and all these six cyber security threats are addressed for better results.

This research paper underscores the urgency of addressing emerging cyber security threats through the development of futuristic techno-legal standards and frameworks. By bridging the gap between technology and law, organizations and law enforcement agencies can bolster their defenses against cyber crimes and improve conviction rates.

The findings of this study highlight the need for proactive measures to combat ransomware attacks, mobile banking malware, AI-enabled attacks, insider threats, and social engineering. Embracing innovative technologies, such as AI, blockchain, and quantum computing, while developing robust legal frameworks to govern their use, is crucial to creating a more secure digital landscape.

International cooperation and harmonization of legal standards are essential to effectively prosecute cyber criminals and deter future attacks. By working together across borders and sectors, stakeholders can create a more resilient and secure digital ecosystem that fosters innovation, protects individual rights, and upholds the rule of law. As the cyber threat landscape continues to evolve, it is imperative that cybersecurity efforts keep pace. By investing in research, fostering collaboration, and adapting to new challenges, we can build a future where digital systems are secure, resilient, and trusted by all.

*****

VI. References

1. Cybercrime and Cybersecurity Paul Watters, 2023
2. Advanced Penetration Testing: Hacking the World's Most Secure Networks Wil Allsopp, 2017
3. Mastering Hacking: The Art of Information Gathering & Scanning Harsh Bothra, 2019
4. Cyber-Crime and the Challenges of Prosecution and Prevention. https://ijlmh.com/wp-content/uploads/Cyber-Crime-and-the-Challenges-of-Prosecution-and-Prevention.pdf
5. Books and reports such as ENISA (European Union Agency for Cybersecurity). (2023). Identifying Emerging Cyber Security Threats and Challenges for 2030. https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf
6. Books and reports such as Imperva. (n.d.). Cybersecurity Threats Types & Sources. https://www.imperva.com/learn/application-security/cyber-security-threats/
7. Books and reports such as RAND. (n.d.). The Future of Cybercrime in Light of TechnologyDevelopments.https://www.rand.org/content/dam/rand/pubs/research_reports/RRA100/RRA137-1/RAND_RRA137-1.pdf
8. United Nations Office on Drugs and Crime (UNODC). (n.d.). Cybercrime Module 2 Key Issues https://www.unodc.org/e4j/en/cybercrime/module-2/key-issues/references.html
9. IJLMH. (n.d.). A Study on Cyber Crime and its Legal Framework in India. https://ijlmh.com/paper/a-study-on-cyber-crime-and-its-legal-framework-in-india/
10. Manupatra. (n.d.). EMERGENCE OF CYBER CRIMES: A CHALLENGE FOR THE NEWMILLENNIUM.http://docs.manupatra.in/newsline/articles/Upload/4730150C-4A12-4EBA-8CAF-F1146FDD5657.pdf
11. International Journal for Multidisciplinary Research (IJFMR). (2025). Cyber Laws in India: https://www.ijfmr.com/papers/2025/2/37346.pdf (2021).
12. Analyses of Cybercrime Regulations Falling behind New Technologies. Journal of SocialScienceshttps://www.researchgate.net/publication/369667892_Analyses_of_Cybercrime_Regulations_Falling_behind_New_Technologies
13. Russo, S., Oliveira, R., & Ramos, I. (2021). The Role of Artificial Intelligence in Enhancing Cybersecurity. International Journal of Artificial Intelligence.