OPEN ACCESS

International Journal of Innovations in Science & Technology

RESEARCH & INNOVATION DIVISION

IJIST

Cybersecurity Legislation Challenges and Remedies

Amna Shahzadi[1], Talha Waheed[2], Hamid Raza Malik[1], Abdul Basit Dogar[1], Kashif Ishaq[1]

[1]Department of Informatics and Systems, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan.

[2]Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan.

***Correspondence**: kashif.ishaq@umt.edu.pk

Citation | Shahzadi. A, Waheed. T, Malik. H. R, Dogar. A. B, Ishaq. K, "Cybersecurity Legislature Challenges and Remedies", IJIST, Vol. 07 Issue. 03 pp 1796-1810, August 2025

Received | June 22, 2025 **Revised |** Aug 03, 2025 **Accepted |** Aug 05, 2025 **Published |** Aug 06, 2025.

The use of the Internet is growing rapidly in every field of life, such as in business, education, entertainment, information technology, the government sector, and sports. The majority of people are using internet services for online businesses and other online activities. Therefore, it is the need of the hour that the online system should be secure enough, and everyone is fully assured about privacy and the protection of their information. A country needs to have an efficient plan to secure its digital information. Different countries have established legislatures to manage cybercrime activities and cyber threats. In this paper, we analyzed the challenges faced by cybersecurity concerning legislation along with their probable solutions. The purpose of this paper is to provide an extensive review of the literature on cybersecurity, including its loopholes, and present the findings of a survey conducted in various organizations regarding cybersecurity. This study also highlights the improvements and the need for future work in the field of cybersecurity. In addition, the mandatory procedures and mitigation techniques to reduce the occurrence of cybercrime have also been discussed.

Keywords: Cyber Security, Cyber Threats, Vulnerability, Cyberbullying, Cybercrime.

Introduction:

The 21st century marks the rise of e-commerce, where almost everyone aspires to bring their ideas online. Consumers increasingly prefer convenient digital solutions, supported by one-click payment options and doorstep delivery services [1]. This has been made possible by widespread internet access, and this distinctive trend has significantly fueled the growth of online businesses [2] Beyond online businesses and social networking, the internet is also utilized by military, financial, and government organizations worldwide to transmit sensitive data across its vast networks. Along with many benefits of the cyber world, it also has some constraints, like cybercrime is at the top of the list [3] The prefix "cyber" is used to denote something related to the information age and the realm of computers. Furthermore, the cyber world poses risks that can compromise or destroy digital information [4] including cyber-attacks, cyber threats, and cyberbullying. Cyber-attacks are internet-based attacks, including acts of deliberate, large-scale disruption of computer networks, especially personal computers attached to the internet by means of certain methods such as viruses, attacks, and hacking etc. Although obtaining someone else's information without their consent is classified as a criminal offense, it remains a common practice that persists worldwide. Hackers try to attack the victim's confidential information and manipulate it. Therefore, it is necessary to protect the system from unauthorized access and achieve confidentiality, integrity, and availability through modern technology, planning, policies, and legislation [5]. On the other hand, cyber threats refer to deliberate or opportunistic malicious activities that exploit weaknesses in systems, networks, or human behavior to steal data, disrupt services, or gain unauthorized access [6]. Combating them requires strong threat intelligence, continuous monitoring, and user awareness [7]. Moreover, Cyberbullying represents the social and psychological dimension of online risks, involving the use of digital platforms to harass, intimidate, or humiliate individuals. This can include spreading false information, sharing private images without consent, or engaging in repeated online harassment. Such actions can lead to severe emotional distress, mental health issues, and even self-harm among victims, particularly children and adolescents [8]. Addressing cyberbullying requires not only technological solutions such as content moderation and reporting systems but also educational initiatives, community support mechanisms, and clear legal frameworks.

The prevention of unauthorized access to information, computers, and networks is known as cybersecurity, and this term refers to the processes and technologies designed to protect networks [9][10]. The main focus of cybersecurity is to protect networks, computers, programs, and data from unintended changes and destruction. However, cyber-attacks are increasing at an alarming rate, making it challenging to secure networks against hackers. The motives driving these attacks vary widely in nature. For instance, a company might attempt to tarnish its competitor's reputation, or a nation might seek to undermine its rival country's economy. Over social media, hackers pretend to be someone else and use fake identities for leisure or personal grudges. Every nation needs to secure its online infrastructure in a way that makes breaches extremely difficult [11] There is an urgent need to establish and enforce strict laws against cybercrime, ensuring they are applied with full authority [12].

Although several studies have examined cybersecurity legislation in individual countries, there remains a gap in systematically comparing laws across different nations while also assessing their practical enforcement. In particular, little research integrates both literature analysis and organizational survey data to evaluate legislative effectiveness, especially in developing countries such as Pakistan. This study addresses this gap by analyzing global cybersecurity laws, surveying financial and non-financial organizations, and proposing remedies for the shortcomings observed in practice.

Methodology:

Research Design:

To complement our literature review, we conducted an exploratory survey to examine awareness, perceived usefulness, and the practicality of cybersecurity legislation in both financial and non-financial organizations.

Sampling Method:

A purposive sampling strategy was employed to target organizations where cybersecurity concerns are most prominent. The financial sector sample included banks and multinational companies, while the non-financial sample focused on educational institutions such as universities and colleges. Due to confidentiality agreements, organizational names are not disclosed.

Inclusion and Exclusion Criteria:

Organizations with an established IT or information management department were included to ensure informed responses. Entities without dedicated IT/security personnel were excluded, as they could not provide relevant insights into cybersecurity practices and legislation.

Questionnaire Design:

The questionnaire was developed based on prior studies on cybersecurity legislation and organizational awareness. It consisted of both closed-ended and open-ended questions covering:

- Awareness of existing cybersecurity laws,
- Perceived usefulness and adequacy of these laws,
- Challenges in implementation, and
- Suggestions for improvement.

Number of Respondents:

A total of 11 organizations participated, including 4 from the financial sector and 7 from the non-financial sector (Table I). Within each organization, responses were collected from IT/security staff and administrative officers directly involved in information management

Table 1. Survey Conducted in Financial and Non-Financial Sectors

Category	No. of surveys	Respondent Roles/Departments
Financial Sector	4	IT Managers, Security Officers, Administrative Staff
Non-financial Sector	7	University/College IT Staff, System Administrators, Academic Administration Officers

Data Analysis:

Survey responses were analysed using descriptive statistics (frequency and percentage distributions) to identify trends and patterns. Open-ended responses were thematically coded to extract qualitative insights regarding challenges and recommendations for cybersecurity legislation.

Results:

The survey conducted across 11 organizations (4 financial, 7 non-financial) produced both quantitative and qualitative insights.

Awareness and Perceived Usefulness of Cybersecurity Laws:

Financial sector respondents reported higher awareness of national and international cybersecurity legislation (75%) compared to the non-financial sector (42%).

However, only 40% across both groups considered the laws "adequate" in addressing current cyber threats, highlighting a perceived gap between legislation and practical enforcement.

Commonly Reported Cyber Threats: Figure 1 and Figure 2 illustrate the distribution of attack tools. Denial-of-Service (DoS) attacks, Trojan horses/botnets, and viruses/worms emerged as the most frequently experienced threats across sectors.

Financial organizations particularly emphasized risks from unauthorized access, email scams, and e-forgery, while educational institutions highlighted phishing, DoS, and spyware attacks.

Motivations Behind Cybercrime:

Financial gain was the dominant motive, especially for identity theft and credit card fraud. Insider threats were a recurring concern within the financial sector, while phishing and social engineering were more common in non-financial organizations.

Implementation Challenges:

Respondents consistently cited weak enforcement, lack of trust in reporting mechanisms, and absence of regulatory compliance frameworks as key barriers.

Over 60% of respondents stated that existing penalties and punishments were not sufficient deterrents.

Comparative Legislative Insights:

Analysis of international laws (summarized in Table 2 and Table 3) shows that while countries like the US, UK, and EU have well-structured frameworks and enforceable penalties, developing nations such as Pakistan and Nigeria face issues of enforcement, awareness, and resource limitations.

Case studies (e.g., Albert Gonzales, Kevin Mitnick) demonstrate that strict enforcement and visible punishments in some nations serve as effective deterrents, a practice that remains limited in Pakistan.

Literature Review of Legislation in Different Nations:

In the physical world, theft occurs when "Property of A is transferred to B; A had it, and now only B has it." In cyber theft, however, "Property is duplicated; A retains it, but B also possesses an identical copy." Countries have established their own sets of legislation to address cybercrimes and developed policies tailored to meet their specific needs.

Implementation of legislation in different countries:

Cybercrime differs from traditional theft in that stolen data is not removed but duplicated, creating unique challenges for legal systems. In response, nations have developed diverse legislative frameworks tailored to their contexts, ranging from sector-specific protections to comprehensive national cybersecurity laws [13]. The following overview highlights how different countries have implemented and enforced these measures**.**

United States:

The U.S. follows a decentralized approach where states enact their cybercrime laws. California's Comprehensive Computer Data Access and Fraud Act criminalizes hacking and data theft, while Texas's Computer Crimes Act addresses hacking and DoS attacks. Broader state-level provisions exist for identity theft, cyberstalking, and cyberbullying, though enforcement remains fragmented [14]. At the federal level, laws remain sector-specific: the Health Insurance Portability and Accountability Act (HIPAA) protects health data, the Gramm-Leach-Bliley Act (GLBA) secures financial information, and the Sarbanes-Oxley Act enforces corporate accountability [15]. The California Consumer Privacy Act (CCPA) strengthened consumer rights, while the Cybercrime Act (2002) and the Can-Spam Act (2003/2004) introduced tougher penalties for cyber offenses and regulated unsolicited emails [16].

United Kingdom:

The UK relies on the Computer Misuse Act (1990) to criminalize hacking and unauthorized access, though it is often seen as outdated. The Data Protection Act (2018) and GDPR safeguard personal data with strict compliance requirements, while the Cybersecurity Information-Sharing Partnership (CISP) promotes public–private intelligence sharing. The Privacy and Electronic Communications Regulations (2003) further restrict spam and unsolicited communications [6].

European Union:

The EU Cybersecurity Act (2019) enhanced the mandate of ENISA and introduced certification frameworks, while the NIS2 Directive expanded cybersecurity obligations. Most recently, the Cyber Resilience Act (2024) established built-in security requirements for connected devices [2].

Canada & Germany:

Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) remains the cornerstone of privacy protection, complemented by the 2010 Cybersecurity Strategy [13] Germany enforces the Federal Data Protection Act (BDSG) and GDPR, alongside the Network Enforcement Act (NetzDG), to combat online hate speech and misinformation [17].

China & Southeast Asia:

China enforces a highly centralized framework through the Cybersecurity Law, Data Security Law, and Personal Information Protection Law (2021), emphasizing surveillance, censorship, and state sovereignty. The Network Data Security Regulation (2024) further institutionalizes deterrence measures [18][19] Vietnam's Cybersecurity Law (2018), Laos's Cybercrime (2015) and Cybersecurity (2017) laws, and Cambodia's Telecommunications Law (2015) prioritize state control, censorship, and surveillance over individual privacy [18].

India & Pakistan:

India addresses cybercrime primarily through the Information Technology Act (2000, amended in 2008), which covers hacking, identity theft, and cyberterrorism. Provisions of the IPC and sectoral laws, such as the Trade Marks Act (1999), also apply [20]. Pakistan's framework evolved from the Electronic Transaction Ordinance (2002) and Electronic Crimes Act (2004) to the Prevention of Electronic Crimes Act (PECA, 2016), which remains the core legislation addressing hacking, harassment, phishing, and cyber terrorism [13].

Singapore & Middle East:

Singapore's Cybersecurity Act (2018) regulates critical infrastructure and promotes public–private cooperation [21]. In the Middle East, Egypt adopted the Anti-Terrorism Law (2015), the Combating IT Crimes Law (2018), and the Personal Data Protection Law (2020), alongside a National Cybersecurity Strategy [4][22]. The UAE relies on NESA and Dubai's Cybersecurity Strategy, Saudi Arabia on the National Cybersecurity Authority (NCA) and Essential Cybersecurity Controls, and Qatar on its National Cybersecurity Strategy (QNCSS) [22].

Nigeria:

Nigeria's Cybercrimes (Prohibition, Prevention, etc.) Act (2015) criminalizes fraud, identity theft, and cyberstalking, while establishing cybercrime units and enhancing forensics. However, enforcement remains a challenge due to resource limitations [9][17].

Table 2. Comparison of Legislatures of Different Nations

Ref	Countries	Laws
[14]	America	California's Comprehensive Computer Data Access and Fraud Act, Texas's Computer Crimes Act,
[15]		National Institute of Standards and Technology (NIST)
[15]		Health Insurance Portability and Accountability Act (HIPAA)
[15]		Gramm-Leach-Bliley Act (GLBA)
[15]		Sarbanes-Oxley Act

[15][21][23]		California Consumer Privacy Act (CCPA)
[16]		Cybercrime Act (2002), Can-Spam Act (2003/2004)
[6]	United Kingdom	Computer Misuse Act 1990, Data Protection Act 2018, and GDPR, Cybersecurity Information-Sharing Partnership (CISP),
[16]		Privacy and Electronic Communications Regulations (2003)
[2]	European Union	EU Cybersecurity Act (2019), Cyber Resilience Act (2024
[13]	Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)
[17]	Germany	Federal Data Protection Act (BDSG), GDPR, Germany's Network Enforcement Act (NetzDG)
[18][19][23]	China	China’s Cybersecurity Law
[19]		Network Data Security Regulation (2024)
[18]	Vietnam	Vietnam’s Law on Cybersecurity (2018)
[18]	Laos	Cybercrime Law (2015) and Cybersecurity Law (2017
[18]	Cambodia	Law on Telecommunications (2015) and a draft Cybercrime Law
[20]	India	Trade Marks Act (1999), some local laws, Information Technology Act, 2000 (amended in 2008),
[13]	Pakistan	Electronic Transaction Ordinance (ETO) 2002, Electronic Crimes Act 2004, Pakistan Telecommunication Act 1996, Cyber Security Council Bill 2014, Prevention of Electronic Crimes Act (PECA) 2016
[21]	Singapore	Singapore’s Cybersecurity Act (2018)
[4]	Egypt	Anti-Terrorism Law No. 94 of 2015, Personal Data Protection Law 151 of 2020, and Combating Information Technology Crimes Law No. 175 of 2018
[22]		Egyptian National Cyber Security Strategy
[22]	Qatar	Qatar National Cyber Security Strategy (QNCSS)
[22]	UAE	National Electronic Security Authority (NESA) & Dubai Cyber Security Strategy (DCSS)

[22]	Saudi Arabia	National Cybersecurity Authority (NCA) & Essential Cybersecurity Controls (ECC):
[9]	Nigeria	Cybersecurity Law
[17]		Nigeria's Cybercrimes (prohibition, prevention, etc.) Act of 2015

Practicality of Legislature in Different Countries:

Most of the companies are reluctant to share any cybercrime data or users' information with the government due to a lack of trust. For instance, in the United States, the Cyber Intelligence Sharing and Protection Act (CISPA) permits companies to share users' information and details of cyber theft with the government as a measure to prevent and address cybercrime. Despite this, organizations often hesitate to report cybercrimes to the government due to concerns over reputational damage and potential loss of customer trust. Similarly, individuals are reluctant to share their personal information and are unwilling to permit any organization to disclose their private data to external entities [17]. Table 2 summarizes the various legislations passed by different countries regarding cybercrime. Also, a few legislations that have been passed by their government and the higher authorities of different countries. However, the implementation of cyber legislation is different in Pakistan.

Pakistani Legislature / Acts for Cyber Crime Prevention:

There are a few ordinances that are present in Pakistan, one of which is the Electronic Transaction Ordinance. According to this the data that is in electronic form, how to deal them. In this, they specify what the customer's duties and authorities are that they can use to this extent, and who is responsible for updating, deleting, and using this information.

Punishments for Cyber Criminals:

Enforcement and implementation of legislation are well built in some countries like the USA, UK, etc., which makes these nations more secure as compared to other countries in the cyber world. Cyber world not only affects the commercial and telecommunication sector but also affects the industry, economy, and public sector [24]. Therefore, in order to defend the country from internal and external terrorism, enforcement and strict applicable legislation are necessary. Apart from the enforcement of cybersecurity to prevent any future crimes, punishments have also been decided upon for those who do not abide by the law. Table 3 illustrates the practical application of cybercrime legislation across various countries by presenting real-world cases of hackers, their criminal activities, associated punishments, and national contexts. This table serves as a valuable resource in cybersecurity by linking academic research with actual incidents, offering concrete case studies for analysis. It sheds light on diverse attack methods such as credit card theft, malware creation, and social engineering, enabling professionals to better understand threat patterns and strengthen defense mechanisms. The documentation of punishments highlights the role of legal frameworks as deterrents, while the inclusion of nations underscores the global nature of cybercrime and the importance of international collaboration. Overall, this table effectively bridges research and practice, making it highly relevant for training, policy development, and awareness initiatives.

Table 3. Practicality of Legislature in Different Countries

Ref	**Name**	**Crime**	**Punishment**	**Nation**
[11]	Albert Gonzales	Stealing app with 130 million credit & debit card numbers	20 years in prison	America
[25]	AlexUdakov, Gribodemon, or Paunch	Primary developer/seller of the SpyEye banking trojan; losses estimated in the	9 years 6 months in U.S. federal prison + 3 years	Russia

		hundreds of millions to financial institutions		
[26]	Kevin Mitnick	possession of several forged identification documents	5 years in prison	America
[25]	Hamza Bendelladj	Co-developer/distributor and botnet operator for SpyEye; theft of online-banking credentials	15 years in U.S. federal prison + 3 years supervised	Algeria
[27]	Kevin Mitnick	High-profile intrusions/social-engineering in the 1990s; widely covered in technical & legal scholarship.	Various sentences, most notably 46 months in prison (1999)	United States

Survey Feedback from Different Sectors:

The cyber world has become integral to both financial and non-financial sectors. For example, the banking system represents the financial sector, while the educational system exemplifies the non-financial sector. Security is imperative for the financial sector. In financial sectors, most of the attacks come from inside the organization, and their rate is continuously increasing [28]. On the other hand, non-financial sectors are not as vulnerable as financial sectors, but still, some level of security must be present.

Importance of cyber security:

Cyber terrorism ranges from simple hacking by computer viruses to causing a terror war in the computer world. Data from different organizations needs to be secure from unauthorized access. Therefore, security plays a vital role in all sectors. However, many financial organizations often assign secondary importance to security, prioritizing other benefits instead. This approach increases the vulnerability of their systems to cyber threats.

Tools for Attacks:

In various organizations, criminals have various types of tools that are mainly used to make the network vulnerable.

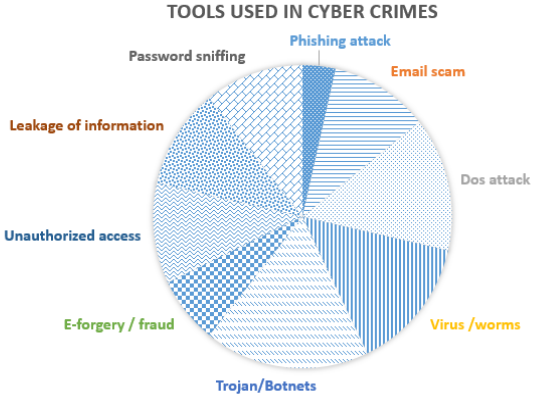

Figure 1. Tools used in cybercrimes

Figure 1 shows different tools that are used to commit cybercrimes. The evaluation of the findings indicates that denial-of-service (DoS) attacks, Trojan horses or botnets, viruses or worms, and unauthorized information leakage are the primary tools commonly employed in such incidents.

The findings highlight that the banking sector is particularly prone to threats such as unauthorized access, email scams, password sniffing, and e-forgery/fraud. On the other hand, the educational sector is more exposed to phishing attacks, DoS attacks, viruses/worms, Trojan horses, botnets/spyware, and information leakage. Figure 2 presents the categorization of these cyber threats, where the *x-axis demonstrates the types of attack tools* and the *y-axis illustrates the probability of occurrence, ranging from 0 (very low likelihood) to 1 (very high likelihood).*

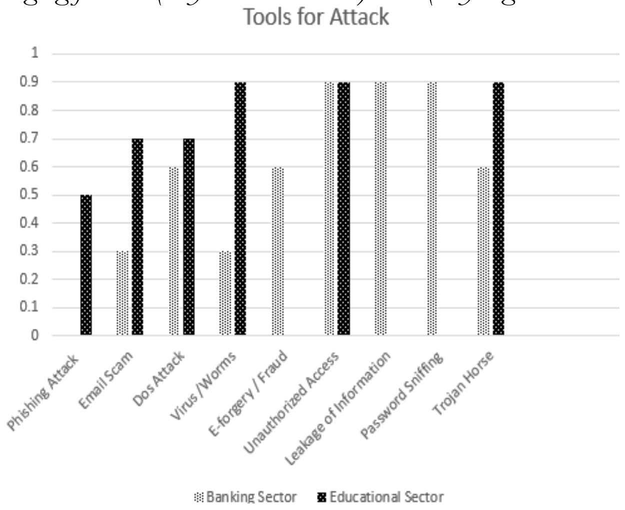

Figure 2. Cybercrimes in the banking and educational sectors

Motivations behind Cybercrimes:

Cybercriminals aim to gain financially through identity theft, credit card fraud, and online banking fraud. While personal online banking has provided customers with convenience, it has also made banking fraud more convenient through online services [28]. Outside financial organizations, cybercriminals often use tactics such as phishing scams to gain access to others' email accounts. On the other hand, a malicious person within a financial organization may use hacking techniques to gain access to internal systems. Financial institutions must implement robust safeguards and monitoring techniques to prevent cybercrime or, at the very least, detect any malicious or suspicious activity as early as possible. Personal identity and credentials can be hacked by attackers to retrieve secret information. Such information may later be exploited for terrorism, blackmail, or other malicious activities. Due to weak law enforcement, individuals often do not fear facing legal consequences [23]. Therefore, it is the need of the day to revise policies and legislation, such that cyber threats are mitigated and criminals are caught wherever they are.

Breakdown of Cyber Legislatures:

Cybercrime can be divided into three phases. The first phase involves identifying the motive behind the crime and determining the tools used to commit it. The second phase focuses on tracing the source from which the crime originated. The third phase is to find out the criticality of the crime that whether it was done unintentionally or deliberately. Here is a brief overview explaining the shortcomings of cyber legislation.

Reasons for committing cybercrimes:

Organizations protect their network and data by using firewalls and intrusion detection and prevention systems. But due to a drastic increase in advanced technologies, new malware has been designed that can bypass the system hardware. Many institutes encounter a problem of unauthorized access by secretly implanting logic bombs and key loggers, which can steal access codes and bypass firewalls and intrusion detection, and prevention systems.

The use of the latest technologies has made network access easy, and humans are a major part of any organization, playing a vital role in maintaining or breaching the security. Errors may also occur during the system configuration phase, often due to negligence, which can enable unauthorized access. Moreover, many organizations lack a dedicated department to manage and secure discarded data. While this data may hold little value for the organization itself, it can be highly valuable to a cybercriminal seeking to cause harm. Hard copies of data are generally thrown away and not permanently discarded. Consequently, a dumpster diving attack by cyber criminals' results in theft of passwords or other secret information of the organization. While some financial organizations burn their data and others do not, there are no legal rewards or punishments regarding the wrong or right handling of the garbage data.

Hurdles for enforcing cyber laws:

The following issues have been found as hurdles for enforcing the cybercrime laws in a country:

Jurisdictional issues:

Jurisdiction authorities are authorities who have official power to make legal decisions and enforce justice. However, there are plenty of laws, but many of them are not implemented. In the Senate, representatives are not fully aware of the methods and consequences of cybercrimes. Inadequate awareness and insufficient records are the main reasons why many countries fall behind in the field of cybersecurity [29].

Thus, jurisdictional issues cause harm to the enforcement of cyber laws by slowing down or completely blocking the enforcement process [30] Thus, there is a need to conduct awareness programs to legislative authorities regarding the importance and criticality of this issue. Also, there is a dire need for cybersecurity experts in jurisdictional departments.

Expertise of criminals:

Skilled cybercriminals often leave no traces of their activities, making it difficult to determine who committed the crime, how they can be held accountable, and what penalties whether imprisonment, fines, or both should be imposed. Furthermore, progress in technology also means progress in malicious software used by cyber criminals. Software tools such as sniffers, backdoors, phishing kits, and keylogger programs are readily available, often accompanied by tutorials, making it easier to launch malicious attacks. Limited knowledge of programming and hacking skills is required to use this software [22].

No regulatory compliance:

Unfortunately, there is no dedicated department in many countries for monitoring the cybersecurity of the private and public sectors and reporting to the government on an annual basis. When a cybercrime is committed by any person or organization, there is no regulatory compliance enforcement to check that the crime has taken place until the victim takes the initiative to report it [31]. There is no such regulatory body to enforce the companies to adhere to the laws, guidelines, regulations, and specifications relevant to their businesses. So that all the organizations are forced to follow it [9] There is an essential need to build a regulatory compliance framework for regulating cyber laws, especially in developing countries. Moreover, cybercrimes cannot be investigated in many countries since there is no law to keep a check on cyber offenses.

How to Make Cyber Legislation Fruitful:

There is an emerging need for cybersecurity, and every country has its cybersecurity laws; however, they do not have a common law that all countries have agreed upon. Similarly, no agreement brings all countries on the same page and deals with the intelligent investigation of cybercrime. The scope of cyber legislation should be sufficiently productive through proper policies and prevention strategies.

Policies:

When addressing cybercrimes, relevant stakeholders must answer certain questions. Where should criminal acts reside in the digital world? What tools/techniques are used for performing the criminal act? Why are malicious activities initiated, or what are the motives behind these malicious activities? Who is responsible for performing malicious acts? We have to find out answers to all these questions and set our policies and strategies for financial as well as non-financial organizations [32].

These policies aim to protect the public and private infrastructure from cyber-attacks to tackle vulnerabilities, and prevent the cyber world from cybercrimes [22] It is now imperative to adopt a global perspective and develop effective cyber strategies to safeguard the digital world [23].

Prevention Strategies:

The most important thing to prevent the increasing trend of cybercrime is through effective prevention strategies. These strategies should be secure, safe, and resilient cyber space [17]. There is a need to suggest some points regarding cybersecurity that will be fruitful against cybercrimes. Firstly, cybercrimes' prevention strategies must deal with confidentiality, integrity, and availability issues along with the misuse of data or information.

Next, computer and anti-virus versions must be up to date on a regular basis with the latest patches and systems to cater to zero-day attacks. After updating policies, it is essential to protect the system from unauthorized access with the help of passwords. These passwords should be changed regularly, with the frequency determined by the sensitivity and confidentiality level of the system's information. Different passwords must be used for login to different accounts, such as bank accounts and email accounts, etc [33]. It should be mandatory to change the default configuration of devices to make them more secure with your policies. Furthermore, credit cards and bank statements should be reviewed regularly by the account holder to keep a check on unusual activities.

Moving further, audit logs must be reviewed, and network traffic must be monitored to keep a check on the irregularity of the network. Intrusion detection and prevention systems are also helpful to resolve these issues, and unauthorized links must be avoided as they may lead to phishing or a DoS attack. Moreover, it is necessary to protect private information from friends and colleagues to prevent social engineering attacks. Expert training and awareness are also necessary to mitigate crimes [34]. Moreover, there is a need for international cooperation that helps in fostering linkages to improve security and for better relations among different nations [3]. Security can also be achieved by using high-technology equipment and specialized investigation units.

Improvements & Recommendations:

There is always room for further improvements. Similarly, in cybersecurity, future work can be done by developing good relations with other countries and building a cyber cell in various nations, as well as by using modern technology. Because cybersecurity is a global problem, it can be solved effectively with coordination, such as:

Fostering Linkages and Building Partnerships:

Knowing the value of fostering cooperation between countries and enhancing their coordination is crucial for cybersecurity [35]. Such collaboration builds trust in governing frameworks and strengthens the use of cybersecurity cooperation among nations [21]. At the same time, building national-level partnerships and creating awareness are equally important [6]. Experts from different nations can work together to establish cybercrime cells, while policies can be developed in consultation with organizational leaders. Public awareness of cyber laws can be promoted through social media, pamphlets, emails, seminars, training, and educational institutions [35]. Establishing these partnerships at both national and international levels not only promotes awareness but also strengthens collective action against cybercrime [21].

Link to Cybersecurity Legislatures:

Cybersecurity legislatures require a stronger alignment between international and national legal frameworks governing cyberspace, particularly in areas such as attribution, accountability, and enforcement. Although instruments like the UN Charter and the Tallinn Manual provide useful guiding principles, they lack binding authority, leaving states dependent on fragmented national legislations [35]. To address these gaps, fostering international linkages, building cross-border partnerships, and promoting public awareness must be pursued alongside efforts to strengthen laws at both domestic and global levels [6] Such an integrated approach can help formalize cyber norms, clearly define state responsibilities, and establish enforceable mechanisms for accountability in cyberspace.

Training and Awareness Raising:

Awareness can be given to users to indicate limitations of use in the cyber world by organizing seminars, distributing pamphlets, emails, etc [36]. Including cyber security awareness subject in the curriculum at the secondary education level will result in awareness amongst the youth about cyberbullying [37]. Cyberbullying occurs among young people. When an adult is involved, it may meet the definition of cyber-harassment or cyber-stalking [23].

Endorse cybercrime technical research:

We should promote technical research to enhance the understanding of cybercrime's causes as well as discover ways to prevent it. For instance, research in intelligence analysis and knowledge management systems has enabled law enforcement agencies to effectively manage various types of criminal and intelligence data, information, and knowledge, which allows them to efficiently analyze large volumes of crime-related information [24]. In the same way, to enhance and support digital productivity across the globe, we need to invest in research and its regulations. Cybersecurity operates in an adversarial, fast-changing environment where threats, technologies, and regulations constantly evolve. Challenges include uncertainty in risks, difficulty in measuring impact, and a tendency to overlook human factors in favor of techno-centric approaches [38].

Need for Robust Standards and Legal Frameworks in Cybersecurity:

To address evolving cyber threats, cybersecurity standards must be adaptive and forward-looking, incorporating emerging risks such as AI-enabled attacks and quantum vulnerabilities. International frameworks like ISO/IEC 27001, NIST, and the Budapest Convention should be expanded to ensure harmonization of laws, stronger cross-border cooperation, and standardized definitions of cybercrime [29]. International standards in cybersecurity are useful as they harmonize laws, ensure cross-border cooperation, and provide structured frameworks for protecting data and combating cybercrime effectively [39]**.** National laws need to integrate privacy-preserving measures, consumer protection, and clearer accountability for tech companies. Additionally, continuous cybersecurity education, awareness programs, and capacity-building for law enforcement should be prioritized to ensure both resilience and global interoperability [14].

Conclusion:

Cybercrime is increasing drastically with the use of mobile phones and other electronic services. Cyber offenders are using modern technologies and knowledge to accomplish illegal activities. To counter such activities, there is a need for information security management systems (ISMS) and appropriate legislation accordingly. Priority to cybercrime legislation as well as enforcement of the law is important. Standards and procedures for reducing cyber risks should be introduced. We also analysed through a survey that financial sectors are usually more vulnerable to cyber-attacks as compared to non-financial sectors. There is a need to recognize a flexible, performance-based, and cost-effective approach for managing cyber risks and control methodologies. The government should be actively involved in passing cybersecurity acts and laws and implementing them. The IT security industry also plays a crucial role in preventing cyber threats and addressing the technical and operational challenges associated with the world.

References:

[1] M. A.-A. M. Al-Amaireh, "The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes," *Rev. Gestão - RGSA*, 2024, [Online]. Available: https://rgsa.openaccesspublications.org/rgsa/article/view/6508

[2] L. A. Bygrave, "The emergence of EU cybersecurity law: A tale of lemons, angst, turf, surf and grey boxes," *Comput. Law Secur. Rev.*, vol. 56, p. 106071, 2025, doi:

https://doi.org/10.1016/j.clsr.2024.106071.

[3] B. Badreddine, “National Cybersecurity: A New Evolving Concept,” vol. 10, no. 1, pp. 433–448, 2025, [Online]. Available: https://asjp.cerist.dz/en/article/269649

[4] M. A. Elokaby, “Development of cybersecurity laws in Egypt and its impact on the judicial system (Opportunities and challenges),” *Int. Cybersecurity Law Rev. 2024 54*, vol. 5, no. 4, pp. 563–584, Oct. 2024, doi: 10.1365/S43439-024-00132-2.

[5] B. S. Mohammad Salem Hamidi, “Designing a Novel Cybersecurity Framework to Prevent Cyber-Attacks with Reference to Least Developing Countries,” *Nanotechnol. Perceptions*, vol. 20, pp. 159–165, 2024, [Online]. Available: https://www.researchgate.net/publication/382026334_Designing_a_Novel_Cybersecurity_Framework_to_Prevent_Cyber-Attacks_with_Reference_to_Least_Developing_Countries

[6] “Evaluating UK Legislation Effectiveness in Prosecuting Cybercriminals and Deterring Cybercrimes: Identifying Areas for Improvement,” *Pakistan J. Criminol.*, no. 4, pp. 701–721, Sep. 2024, doi: 10.62271/PJC.16.4.701.721.

[7] A. Abisoye and J. I. Akerele, “A Practical Framework for Advancing Cybersecurity, Artificial Intelligence and Technological Ecosystems to Support Regional Economic Development and Innovation,” *Int. J. Multidiscip. Res. Growth Eval.*, vol. 3, no. 1, pp. 700–713, 2022, doi: 10.54660/.IJMRGE.2022.3.1.700-713.

[8] A. Kaminska-Nawrot, D. Bienkowska, and J. Falecki, “A Dignity-Based Approach to Children’s Cybersecurity: A Criminal Analysis,” *Eur. Res. Stud. J.*, vol. XXVIII, no. 1, pp. 3–15, 2025, Accessed: Aug. 21, 2025. [Online]. Available: https://ideas.repec.org/a/ers/journl/vxxviiiy2025i1p3-15.html

[9] M. M. A. Adekunle Emmanuel Makanjuola, “STRENGTHENING CYBERSECURITY IN NIGERIA: A HOLISTIC APPROACH,” *Sci. Pract. cyber Secur. J.*, 2025, [Online]. Available: https://journal.scsa.ge/papers/strengthening-cybersecurity-in-nigeria-a-holistic-approach/

[10] M. W. Hodgins, “The perils of cybersecurity regulation,” *Rev. Austrian Econ.*, 2024, [Online]. Available: https://link.springer.com/article/10.1007/s11138-024-00660-4

[11] D. Neufeld, “Computer crime motives: Do we have it right?,” *Sociol. Compass*, vol. 17, no. 4, p. 4, 2023, doi: https://doi.org/10.1111/soc4.13077.

[12] C. Nwabachili, “LEGALITY OR OTHERWISE FOR THE IMPOSITION OF CYBER SECURITY LEVY IN NIGERIA,” *NAUJILJ*, vol. 16, no. 1, 2025, [Online]. Available: file:///C:/Users/VAIO/Desktop/ajol-file-journals_479_articles_295722_682394873c83b.pdf

[13] M. I. Omer Mahmood Watto, “Cyber Law and Cyber Security Policies in Pakistan: A Comparative Study with USA, Canada and Australia,” *Pakistan J. Humanit. Soc. Sci.*, vol. 12, no. 1, 2024, [Online]. Available: https://journals.internationalrasd.org/index.php/pjhss/article/view/1977

[14] I. Elegbe, “CYBERCRIME LEGISLATION: A COMPARATIVE ANALYSIS OF LEGAL FRAMEWORKS, POLICY RESPONSES AND RECOMMENDATIONS,” *Int. J. Educ. Soc. Sci. Res.*, vol. 7, no. 2, 2024, doi: https://doi.org/10.37500/ijessr.2024.7211.

[15] J. Hiller, K. Kisska-Schulze, and S. Shackelford, “Cybersecurity carrots and sticks,” *Am. Bus. Law J.*, vol. 61, no. 1, pp. 5–29, Mar. 2024, doi: 10.1111/ABLJ.12238’)).

[16] A. R. Mehrdad Falahi, “The Concept of Legislative Criminal Policy in The Blue of Cybercrimes,” *Int. J. Adv. Res. Humanit. Law*, vol. 1, no. 4, pp. 104–113, 2024, doi: 10.63053/ijrel.36.

[17] K. I. Enver Buçaj, “The need for cybercrime regulation on a global scale by the international law and cyber convention,” *Multidiscip. Rev.*, vol. 8, no. 1, p. 1, 2025,

[Online]. Available: https://malque.pub/ojs/index.php/mr/article/view/5348

[18] D. P. K. Shikha Vasishta, "Comparative Trajectories Of Cybersecurity Legislation In Mainland Southeast Asia And China," *Migr. Lett.*, vol. 21, 2024, [Online]. Available: https://migrationletters.com/index.php/ml/article/view/7768

[19] G. F. A. Waqas Abdullah, "Analyzing China's Cybersecurity Posture Under Cyber Deterrence Theory: Reshaping Indo-Pacific Security Landscape (2020-2024)," *Res. J. Soc. Aff.*, vol. 3, no. 4, p. 6, 2025, [Online]. Available: https://rjsaonline.com/journals/index.php/rjsa/article/view/265

[20] R. R. Megha Ojha, "Combating Cybercrime: A Study on Problems, Preventions and Cyber Laws of India," *Eur. Econ. Lett.*, vol. 41, no. 1, 2024, [Online]. Available: https://www.eelet.org.uk/index.php/journal/article/view/1220

[21] L. Qudus, "Cybersecurity governance: Strengthening policy frameworks to address global cybercrime and data privacy challenges," *Int. J. Sci. Res. Arch.*, vol. 14, no. 1, pp. 1146–1163, Jan. 2025, doi: 10.30574/IJSRA.2025.14.1.0225.

[22] S. N. Othman, A. M. Jawad, R. Hameed, R. T. Kawad, and D. Khlaponin, "The impact of cybersecurity law in the middle east," *Encuentros*, no. 23 (enero-abril), pp. 392–420, Jan. 2025, doi: 10.5281/ZENODO.14291287.

[23] Emmanuel Ok, "The Impact of Cybersecurity Laws on Legal Procedures and Case Law," *ResearchGate*, 2025, [Online]. Available: https://www.researchgate.net/publication/387625093_The_Impact_of_Cybersecurity_Laws_on_Legal_Procedures_and_Case_Law

[24] O. V. G. Olena Sviatun, "Combating Cybercrime: Economic and Legal Aspects," *WSEAS Trans. Bus. Econ.*, vol. 18, pp. 751–762, 2021, doi: 10.37394/23207.2021.18.72.

[25] E. C. and R. Mcardle, "The Evolution of Cybercrime and Cyberdefense," *Trend Micro*, 2018, [Online]. Available: https://documents.trendmicro.com/assets/white_papers/wp-evolution-of-cybercrime-and-cyberdefense.pdf

[26] S. T. L. Robert W. Gehl, "Social Engineering: How Crowdmasters, Phreaks, Hackers, and Trolls Created a New Form of Manipulative Communication," *MIT Press*, 2022, doi: https://doi.org/10.7551/mitpress/12984.001.0001.

[27] B. Wible, "A site where hackers are welcome: Using hack-in contests to shape preferences and deter computer crime," *Yale Law J.*, vol. 112, no. 6, pp. 1577–1624, 2003, doi: 10.2307/3657453.

[28] A. I. A.-A. Sara Al-Bassam, "The Significance of Cybersecurity System in Helping Managing Risk in Banking and Financial Sector," *J. Xidian Univ.*, vol. 14, no. 7, 2020, [Online]. Available: https://www.researchgate.net/publication/337086201_The_Significance_of_Cybersecurity_System_in_Helping_Managing_Risk_in_Banking_and_Financial_Sector

[29] M. J. Ali, "Cybercrime and Cybersecurity: A Critical Analysis of Legal Frameworks and Enforcement Mechanisms," *Bharati Int. J. Multidiscip. Res. Dev.*, vol. 2, no. 8, pp. 137–154, Oct. 2024, doi: 10.70798/BIJMRD/020800017.

[30] M. M. and S. Erickson, "Changing Today's Law Enforcement Culture to Face 21st-Century Threats," *Herit. Found.*, 2011, [Online]. Available: https://www.heritage.org/homeland-security/report/changing-todays-law-enforcement-culture-face-21st-century-threats

[31] Guedouari Fatma Zohra . Allouache Mehdi, "The Role Of Cybersecurity In Combating Cybercrime In Algeria: Prospects And Challenges," *Rev. Sci. Hum.*, vol. 36, no. 2, pp. 347–358, 2025, [Online]. Available: https://asjp.cerist.dz/en/article/273427

[32] J. M. Inês Sousa Guedes, "Explaining fear of cybercrime: A focus on interpersonal and property cybercrime differences," *Eur. J. Criminol.*, vol. 22, no. 4, 2025, doi:

https://doi.org/10.1177/14773708241312820.

[33] N. Z. H. Chee Lee Chong, "Secure File Sharing System with Strong Password and One Time Password Authentication," *J. Comput. Res. Innov.*, vol. 10, no. 1, p. 3, 2025, doi: https://doi.org/10.24191/jcrinn.v10i1.500.

[34] D. K. Sunitha Prabhu, "Beyond the direct impact of sanctions and subjective norms in cybersecurity," *Inf. Comput. Secur.*, 2025, doi: 10.1108/ICS-04-2025-0148.

[35] and M. Q. O. Issn, S. Gul, W. Malik, Gohar, "Cybersecurity and sovereignty: the role of international law in governing state behavior in cyberspace," *Policy J. Soc. Sci. Rev.*, 2025, [Online]. Available: https://www.researchgate.net/publication/392373086_cybersecurity_and_sovereignty_the_role_of_international_law_in_governing_state_behavior_in_cyberspace

[36] A. N.-F. Anant Kumar Verma, "Realigning Academic Cybersecurity Research With Industrial Needs in Cyber-Physical Systems," *IEEE Open J. Ind. Electron. Soc.*, vol. 99, pp. 1–9, 2025, doi: 10.1109/OJIES.2025.3593689.

[37] M. Grimland *et al.*, "Cyberbullying Victimization and Suicide Attempt Among Adolescents: A Cross-National Comparison," *Int. J. Environ. Res. Public Health*, vol. 22, no. 3, Mar. 2025, doi: 10.3390/IJERPH22030385,.

[38] and S. M. F. Julie M. Haney, Clyburn Cunningham IV, "Towards Bridging the Research-Practice Gap: Understanding Researcher-Practitioner Interactions and Challenges in Human-Centered Cybersecurity," *Natl. Inst. Stand. Technol.*, 2024, [Online]. Available: http://usenix.org/conference/soups2024/presentation/haney

[39] A. N.-F. Anant Kumar Verma, "International Journal for Conventional and Non-Conventional Warfare Cybersecurity and Islamic Law: Navigating the Challenges of the Digital Age," *IEEE Open J. Ind. Electron. Soc.*, vol. 99, pp. 1–39, 2025, doi: 10.1109/OJIES.2025.3593689.