STM JOURNALS

International Journal of
Information Security Engineering

ISSN: 3049-1150
Volume 4, Issue 1, 2026
January–June
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

The Dark Side of Technology: Addressing the Rise of Cybercrime and Data Breaches

V. Basil Hans[1,*]

Abstract

In the digital age, technological advancements have brought about remarkable improvements in communication, business, and daily life. However, these innovations have also given rise to a darker side of the tech world: an increase in cybercrime and data breaches. This article examines the growing threats posed by malicious actors, including hackers, cybercriminal syndicates, and state-sponsored entities, who exploit vulnerabilities in digital systems. It explores the wide-reaching impacts of cybercrime, from financial loss and identity theft to national security risks. The article further highlights the challenges organizations face in safeguarding sensitive information and the escalating frequency of data breaches, which affect millions of individuals worldwide. With an emphasis on current cybersecurity trends, legal frameworks, and technological advancements, this article offers insights into the strategies and best practices needed to mitigate risks and protect personal and corporate data in an increasingly interconnected world.

Keywords: Cyber, cybercrime, cyberspace, interconnected world, security

INTRODUCTION

The rise of cybercrime and data breaches in the modern-day digital landscape is ushering in dark clouds into the world of emerging technologies, which were hailed not so long ago as transformative. It can only take a couple of clicks for a cybercriminal group to gain access to your smartphone, personal data, financial information, login credentials, etc., seeing everything from your Facebook or LinkedIn profile to what you shared with the tech giants. Moreover, cyber criminals are becoming more organized, powerful, and smart. Every year, billions of dollars are lost because of cyber activities, and this tendency is growing rapidly. In fact, cases in which all funds of companies and individuals in their bank accounts are withdrawn in a millisecond by cyber criminals are no longer news. Ultimately, it has gone viral, such a notion as 'I was hacked.' It is happening in reality. This problem is already global, affecting both developing and developed countries. However, technology and IT-related solutions are at the heart of organizations' operations and processes and are essential for a large share of services across the economy. Booming digitization also means more exposure to threats, such as data breaches and cybersecurity threats. Most data breaches occur because of technological vulnerabilities and hacking activities. IT stacks and implementations with widely vulnerable points that are in demand for quicker modernization. Additionally, the increased use of different technologies is also controlled by humans. Therefore, the probability of cyber threats is growing, together with an increase in human error. As mentioned previously, it is vulnerable. More attention to such threats is needed, and this review can lay the groundwork for following the issue and fostering a secure digital environment [1].

***Author for Correspondence**
V. Basil Hans
E-mail: vhans2011@gmail.com

[1]Research Professor, Department of Management and Commerce, Srinivas University, Mangaluru, Karnataka, India

Received Date: March 14, 2025
Accepted Date: September 03, 2025
Published Date: March 26, 2026

Citation: V. Basil Hans. The Dark Side of Technology: Addressing the Rise of Cybercrime and Data Breaches. International Journal of Information Security Engineering. 2026; 4(1): 6–15p.

REVIEW OF LITERATURE

The literature surrounding the dark side of technology, particularly in relation to cybercrime

and data breaches, reveals a complex interplay of factors that contribute to the rise of these phenomena. The evolution of cybercrime as a global issue is underscored by the foundational work of Hewana (2025) [2], which contextualizes cyber-related crime within the broader frameworks of globalization and modernization. This article highlights the transnational nature of cybercrime, emphasizing the vulnerability of individuals, especially those who may not recognize or know how to respond to cyber threats due to their lack of understanding of social media practices.

Abdulai (2016) [3] builds upon this foundation by investigating the fear associated with cybercrime victimization, particularly among students. His work examines the characteristics of various cybercrimes, such as credit and debit card fraud, and the implications of the transformative impact of cyberspace on criminality. The fear of cybercrime, although not as extensively studied as conventional crime, is rising, prompting further inquiry into socio-criminological theories that seek to explain this phenomenon.

Xiaolin (2017) [4] further elaborated on the vulnerabilities inherent in computer networks, stressing the necessity of a multistakeholder approach to combat cybercrime effectively. Their examination of the internal threats posed by employees underscores the need for organizations to address both external and internal security challenges. McDaniel (2018) [5] amplifies this discussion by revealing the staggering economic costs of cybercrime, particularly fraud, and the low-risk environment that cybercriminals exploit owing to the anonymity of the digital sphere.

The research by Porcedda and Wall (2019) [6] introduces a critical examination of the evolving tactics employed by cybercriminals, particularly in the context of big data. They identified a significant shift in attack vectors, highlighting the increasing prevalence of data breaches and the commodification of stolen data within deep web markets. This trend reflects the broader implications of technological advancements, as the rise of cloud computing has facilitated both legitimate business operations and cybercriminal activities.

Pärn and Edwards (2019) [7] addressed the national security implications of cyber threats, citing incidents such as the WannaCry ransomware attack as examples of sophisticated strategies employed by cybercriminals. Their work emphasizes the challenges of reporting and understanding the anonymity that cyberattacks afford perpetrators. Elizabeth Cannon (2019) [8] takes a more organizational perspective, analyzing the impact of data breaches on businesses and the importance of understanding the underlying causes of such attacks to enhance data protection strategies.

Ertan et al. (2020) [9] delved into the human element of cybersecurity, revealing that a significant proportion of breaches are attributable to inadvertent human error. Their findings highlight the importance of cultivating a culture of cybersecurity awareness within organizations, which was echoed by Uchendu et al. (2021) [10] in their systematic review of cybersecurity culture. They emphasized the need for robust security policies and practices to foster a proactive stance against cyber threats.

Edwards et al. (2022) and Peersman et al. (2022) [11, 12] contribute to the understanding of cybercriminal motivations and characteristics, identifying common traits among offenders and the socio-technical factors that influence their behavior. Their research underscores the necessity for practitioners to adapt to the evolving landscape of cybercrime, particularly as organized crime and cybercrime-as-a-service become more prevalent.

Akter et al. (2025) [13] argued for a comprehensive approach to cybersecurity awareness, advocating for continuous training and education to equip individuals with the knowledge necessary to navigate the complexities of the digital economy. Finally, Buil-Gil et al. (2025) [14] addressed the measurement challenges associated with cybercrime, emphasizing the urgent need for reliable data to inform prevention strategies and understand the prevalence of cybercriminal behavior in an increasingly connected world.

Collectively, these articles illustrate the multifaceted nature of cybercrime and data breaches, highlighting the importance of understanding the interplay between technology, human behavior, and organizational practices in addressing these pressing issues.

HISTORICAL EVOLUTION OF CYBERCRIME

It is easy to underestimate the ingenuity and tenacity of cyber criminals, especially in the face of the most recent high-profile cyber breach. Cybercrime has a historical evolution that has closely mirrored the development of new computer technologies that were created over the last half of the second millennium. From relatively trivial schemes in the early 1970 s involving the theft of long-distance service, or "phone phreaking," services, steadily more sophisticated techniques have emerged to match the technological developments of the times. The historical perspective of cybercrime is important, both because it reveals clearly repeating patterns in offender motivations and techniques, as well as to better appreciate the adversary that the user faces today.

Historical Perspective

There have been six significant milestones in the development of cybercrime. The first was the emergence of the first widely distributed virus in 1982. The first worm emerged quickly in 1988. In 1989, the theft of $70 million from financial institutions was a complaint. In 1996, the phenomenon of "denial of service" denial of service attacks was a complaint. Subsequent major milestones have included the "I Love You" virus that exploited the perceivably safe mode of communication, or email, and most recently the compromise of the infrastructure of the fourth estate, the press, as exemplified by the infamous breach of Sony's computer networks in 2014 [5]. There are many more low-visibility, but serious incidents throughout all sectors of the economy, education, defense, healthcare, and government, which indicate a long-term and ongoing dynamic that began in the late 1980 s, and continues to advance as rapidly as the technology that is its target.

The initial response of law enforcement was, for the most part, a bordering tragedy. Traditional conceptions of criminal behavior, investigation, and intelligence were quickly shown to be woefully unequipped to cover this new phenomenon. The same adaptation, in fits and starts, that offenders who have exploited new technology have applied to those combating cybercrime, and many early countermeasures were quickly negated [15]. Analogously, low-level arms races began and steadily intensified. Early offenders were typically malfeasant hobbyists or otherwise well-intentioned; if fouled, experimenters were typically teenagers with too much free time. The nature of the motives quickly broadened, as did the mechanisms employed.

Early Instances of Cybercrime

Remarkable incidents of cybercrime serve as a testament to its evolution into legitimate threats. On March 6, 1981, a security breach was discovered at the Los Alamos National Laboratory in New Mexico, US. This episode marked one of the first acknowledged instances of cyber espionage [16]. A storage disk was found on the photocopier. Upon examination, it appeared to contain file listings from two computers in different areas of the research facility. This incident laid the foundation for the age of cybercrime. The story begins with the birth of ARPAnet in the 1960s and the early 1970s, the progenitor of the modern internet. This new technology is invaluable to the fields of industry and academia, prompting its rapid adoption. Engineers, professors, and students alike took an interest in computer networks, each using them in their own way. Even in these nascent stages, it was not lost on some individuals that this novel medium could be utilized for illicit purposes. They have adopted ingenious techniques, often exploiting poorly understood network protocols, loopholes in security measures, and the informality of the network. The first cases of cybercrime were born, and, in turn, digital security had to evolve. The first instances serve as an important timeline for recognizing and understanding the threats that are now faced. These stories are notable not just for their inventiveness in crimes produced with new technology, but also for the rudimentary security regulations that prompted crimes and made them so successful. The individuals of these stories acted alone, often for the thrill of seeing how easily they could manipulate this new digital cipher of the world.

TYPES OF CYBERCRIME

The use of computers and networks as tools to commit crimes has given rise to a new category of offenses, known as cybercrime. Cyber threats worldwide converge on some critical issue areas. These include identity theft, credit/debit card fraud, intellectual property rights violations, online harassment, software piracy, computer viruses, and other cyber malice. There are lots of risks with the internet, otherwise known as cyber threats, and these are what cybersecurity seeks to address; it is all the attempts by an unauthorized person to gain access to data, which is not limited to checking accounts, credit cards, health care, and other confidential information [15].

Cyber threats are constantly emerging, making it difficult to keep up to date on the latest threats and how to best protect the computers and networks that connect them. It is important to be aware of potential criminal and civil liabilities for any activity conducted over the internet. Such crimes include cyber harassment, violation of privacy, cyberterrorism, cracking, and cybersquatting. Cyberharassment is a distinct form of cybercrime. Although it is less common today than other cybercrimes, it is nevertheless deserving of attention. It can take many attractive forms in cyberspace, some of which may not be found in nature. Harassment is generally considered to belong to the category of nuisance crimes. Harassment and stalking via the internet have enabled new methods for harassment that are unique to cyberspace. Harassment is a type of interaction that is intended to be disturbing, frightening, or burdensome. It can include email, instant messages, and attachments. There are very thin lines between what is actionable and what does not cause many email harassment cases and other online cases. Harassment also encompasses intentionally and persistently putting another person in fear of life, liberty, or safety.

Malware and Ransomware

The increase in the number and sophistication of cybercrime and data breaches could be staggering. The public sector, government, and individuals lost a total of due to incidents in January. The impact of cybercrimes and cyber incidents may spread rapidly and drastically damage an individual's personal, professional, and social life. The printing and advertising of research-based preventive and informative articles are ineffective because the field of cybersecurity is constantly and rapidly advancing for obvious reasons.

Malware is defined as software that performs malicious and unwanted functions on a computer system, with various effects. Malware primarily functions to damage, obtain unauthorized access, and violate a user's privacy. The general purpose of malware is to facilitate future advanced attacks, such as espionage, cybercrime, identity theft, and botnet identification. In the following computation plan, malware is classified according to its specific type, capabilities, activities, aims, and characteristics. Ransomware is selected as part of malware because it is increasingly powerful and common in cybercrime. Ransomware encrypts files on a user's system and demands payment to decrypt them. Successful ransomware programs may enable users to gain knowledge of the ransomware type and learn to remove it. Cybercriminals use increasingly sophisticated methods, including malware, to exploit vulnerabilities and security to obtain sensitive data in personal and institutional environments within society. As a result, it is unsustainable to craft a comprehensive informational model with a great variety of new developments in tactics. Domain Name System (DNS) spoofing, browser hijacking, adware, malware variants, cyber espionage, hacking, and more malware topics.

DATA BREACHES: CAUSES AND CONSEQUENCES

Corporate data breaches reflect a new societal need and problem, as technology plays a critical and intimate role in personal and professional activities. This highly interconnected environment of social media, smartphones, computers, chromecasting, gaming, and other passive and active technologies ensures the constant surveillance and usage of everyday subjects. However, there are reality-type dangers and threats in this dark matrix of electronics. Those in the US are twice as likely to have their identity stolen as they are to get in a car accident, with nearly 2,500 data breaches in the US in 2018

[17]. These cyberattacks can have devastating consequences for millions but also have a long-term negative effect on any future internet or technology-supplied businesses.

There are many root causes of data breaches, but they can mostly be summarized as human error, system vulnerabilities, and inadequate security measures. Most data breaches are the result of phishing attacks. Employees are often trained to be cautious about email, but not about other forms of electronic communication. Thus, spear/phishing attacks succeed by gaining information from seemingly harmless avenues. A killer resume could have been too successful in advertising a worker, allowing the hacker to customize the phished link. Employees often do not distinguish between personal and work emails, allowing for the beginnings of the hacker's incursion. Given access to the corporate directory, the hacker then creates fake websites, feasible as corporate domain names follow the pattern companiesecurity.companiesname.com. Directors of broader entities can be of particular importance, as hackers obtain user information through social engineering or by using online password recovery forms to input personal information. It is often that the security questions are 'What is your mother's maiden name?' as are the answers. Evidently, this can be observed in the public domain. A further issue arises in unpatched vulnerabilities and unused security features, such as the target breach that occurs in an Heating, Ventilation, and Air Conditioning (HVAC) system. Attacks on Facebook resulted in it adopting compulsory Secure Sockets Layer (SSL) security, which went unused by countless sides. The ease-of-use encouraged digital criminals to use the package, resulting in lasting negative effects on internet security, user licensing, and web usage. Data breaches provide hackers with unprecedented access to data; recent surveys estimate that personal health data sells for at least $250 per record. Finally, even if the data were not sold, merely stolen from war-dialing, it can encrypt information, tampering with medical and treatment services.

THE ROLE OF TECHNOLOGY IN FACILITATING CYBERCRIME

Technology has dramatically changed the world over the decades by improving communication, commerce, and transportation. However, as technological innovations have unfolded and advanced in the past two decades, society has also seen a shift in power dynamics that has culminated in new ways of conducting business and everyday life. This has paved the way for a darker side of technological advancement: the rise of cybercrime and data breaches [18]. In the past, committing large-scale crimes such as syndicated cybercrime required substantial resources. However, in recent years, this requirement has significantly changed because of the internet, cloud computing, and the prevalence of Internet of Things (IoT) devices. Many technologies have been developed with the best intentions, but this has not helped prevent the unintended use of those technologies for criminal activities [19]. Policymakers and law enforcement must review both present and emerging technologies to design adequate legal and policing strategies to mitigate and deter cybercrime. This need is exemplified through the discussion of various technologies that have been lauded as ground-breaking; however, they have also fundamentally shifted the criminal landscape in favor of cyber criminals, and how certain high-profile cybercrimes could have possibly been prevented were the flaws in these technologies to be proactively addressed. Recent and potential future developments in technology are then reviewed, illustrating that technology continues to develop in ways that favor cyber criminals. It is argued that stakeholders involved in the fight against cybercrime need to be proactively engaged in current and emerging technologies to inform legal and technical preventive and detective endeavors.

CYBERSECURITY MEASURES AND BEST PRACTICES

No one could have predicted the astronomical shift in how we conduct our personal and professional lives since the outbreak of the global pandemic. Remote offices and logins have created a perfect recipe for cyber threats. Cybersecurity is rapidly becoming the most critical aspect of maintaining a functional environment for businesses and individuals. There are many strategies that individuals and organizations can adopt to protect their data and systems and to combat cybercrime more effectively. Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks [20]. A successful cybersecurity measure encompasses a multi-layered approach to security. A well-thought-out security strategy leverages various tools and

effective technologies and regularly trains and educates employees on best practices. Proactive monitoring, regular threat assessments, and a well-documented incident response plan are critical for maintaining an effective security stance [13]. Together, these layers function in unison to prevent, monitor, detect, and respond to internal and external threats. Three possible types of attacks are ransomware, an attack that locks a computer system and demands payment to release it, identity theft, and an attack that targets a person by using keyloggers to capture keystrokes and steal personal information. In ransomware situations, robust data backup practices are vital because, in the event of an attack, data can be restored without the need to pay the ransom. Food and Drug Administration-approved antiviral software should be installed on all computers and updated regularly as an added security measure. Installation of hardware firewalls is also important. Awareness and training for employees are also important, as human error is currently the greatest cyber risk. Email and online security procedures should be followed vigorously, and employees should undergo regular cybersecurity training. Strengthening login authentication by adding second-level authentication is another preventive measure to which ownership should adhere. Responsible password management practices involve employing password management software, the use of passwords of at least 12 characters, including uppercase and lowercase letters, special characters, and numbers, and a password should be unique for each account. Malware, phishing, and data breaches can be avoided if these practices are followed. The nature of cyber threats is constantly evolving; therefore, strategies and protections must remain in a state of continuous improvement and evolution.

Encryption and Authentication

Encryption has become an important factor for the protection of all data and information being stored online [21]. Here is the importance of encryption, and the types of methods encryption can be used today. Encryption protects sensitive information, such as passwords, files, and credit card numbers, by transforming the original information into a baffling set of random data that is almost impossible to decode without the right key. Information travels through the internet as a series of packets that can be easily intercepted or hacked. To negate this problem, all internet traffic must be encrypted. Email was one of the early methods of internet communication and was notoriously bad for having no encryption. Blockchain makes it almost impossible to hack into and alter the information, as it ensures that the information in one block matches the previous block. With hackers getting smarter every day, it is only a matter of time before the old encryption can be hacked. With the introduction of quantum computing, hackers may no longer require years to brute force using modern encryption meters [22]. Confidential information can be protected using encryption, which is the process of converting data or information into code to prevent unauthorized access. It is almost impossible to decode or crack random data without the correct key. The system uses hardware embedded in the device to store unique personal certificates used during the SSL/TLS sessions. Each website's contact with the device will generate a unique session certificate, which will be stored safely on the device and can only be deciphered if the session certificate is acquired by the vileness. Precautionary informative measures must be followed to ensure the safety of the information when transmitting data to the device. A fair distance must be maintained when using a device in a public area so that wireless connections or dots can easily be traced back to the respective devices. In areas of high security, all camera devices must be avoided, as the camera uses visual coverage to track a person or an item. When using a shared computer, the device should not allow the storage of cookies or browser history. There are two types of anonymity protection devices connected to the internet. One method is to convert Ethernet data packets into a single, meaningful Internet Protocol (IP) address or tearing between every search and website transport. Devices use a unique rotation and bulb setup, where every device can use multiple IP addresses to have its search terms spread out and shared between several IP addresses.

LEGAL AND ETHICAL CONSIDERATIONS IN CYBERSECURITY

When considering cybersecurity issues, legal and ethical problems seem to persist and provide a constant stream of debate and discussion. This section explores some of the legal and ethical traps that cybersecurity professionals must be wary of, starting with the laws and regulations that make

cybersecurity possible in the first place. It is instructive to consider the compliance requirements imposed on an organization; for example, a hospital will have many regulations governing how it stores data [23]. For cybersecurity professionals, compliance with sector-specific laws and regulations is likely a chief concern in day-to-day operations. Importantly, it is worth remembering that the ability to enforce data protection often relies on users' consent for certain data collection and storage practices. In an era of exploding digitization of everyday activities, this poses questions regarding the boundaries of consent and the right not to consent to certain data practices [24]. In such situations, cybersecurity endeavors pose new and potentially unprecedented threats to the consent and privacy of individuals. By their nature, security measures to protect a user's data may also impinge on end-user rights. One of the biggest concerns in promoting data protection regulations is their implementation and enforcement. At the heart, laws and regulations often conflict with security measures, and cybersecurity professionals may find themselves in an ethical Catch-22. Failure to take securitization measures might put user data at an unacceptable risk; however, these measures may result in legal and ethical breaches. A corollary of this is that there will always be "bad" cases in cybersecurity; the matter of professional ethics will be how these cases are handled. The following case studies will show both the implications of non-compliance with laws and regulations and the ramifications of the ethical boundary being breached. At its core, the data protection law is nothing but a data protection practice. It is of paramount importance to construct a strong ethical framework for cybersecurity practices. Further, the landscape is constantly evolving as new technologies present new issues, meaning that cybersecurity professionals must remain constantly informed and adaptive to the sometimes-conflicting demands of the law. Given the central importance of the collection, storage, processing, and distribution of data in cybersecurity, it is a truly paramount concern that a robust ethical responsibility is taken up by all in the field.

INTERNATIONAL COOPERATION AND CYBERSECURITY

Globalization and the desire to acquire intellectual property or state secrets have spurred the growth of cybercrime worldwide. Developed nations tend to be the primary nations to both consume and develop new technologies and are therefore exposed to cyber thieves. Because electronic information moves rapidly between countries, the suppression of cybercrime is less effective when nations act individually. Legal jurisdictions frequently end at a nation's borders and differ in what is carelessly allowed in cyberspace, as well as in how to punish transgressors. New cyber threats can quickly develop to challenge even the most prepared nations; however, when nations collaborate on cybersecurity efforts, they can effectively manage cyber threats [25]. National cybersecurity strategies are an amalgamation of efforts to mitigate existing cyber threats and risks, while promoting proper conduct in cyberspace. Since no nation can be 100% secure, a deeper investment is in incident response and recovery from cyberattacks. Nigeria is just one country that exemplifies this global need, and, as of 2017, it has resorted to using Interpol (International Criminal Police Organization) as a cooperating party. Co-organized by Interpol and International Telecommunication Union (ITU), workshops were held to improve national and international capabilities in combating cybercrime, including investigations, forensics, and regional and international cooperation. Drawing from detailed case study observations, the effectiveness of such collaborative measures was demonstrated. Broad types of measures taken in anticipation of a possible disaster or attack include improving legislation, increasing public awareness, enhancing education, and media measures aimed at the generalization of global cybersecurity policies. The transnational collaborative efforts of three, four, and more countries are also explored using additional case studies, including no-confidence strategies.

FUTURE TRENDS AND CHALLENGES IN CYBERSECURITY

Introductory paragraphs investigate some basic reasons for changes in security and privacy over decades, followed by a literature review of how the next ten years in security and privacy have been predicted. The methodology adopted is then detailed, and a description of the context in which the research was conducted is provided. The results of the survey are then described first and then in more detail, highlighting common themes and focusing specifically on those results that inform us of the next step. Four vignettes indicative of wider survey findings were presented. A discussion of the impact of

these results in stimulating research and improving practice is then given, paying particular attention to issues of socio-technical trade-offs and future research requirements. Finally, the work is reflected on, and conclusions are drawn by considering the next iteration of work in this area [26].

RESULTS AND DISCUSSION

The rapid integration of advanced technologies into everyday life has undeniably led to significant benefits across various sectors, from health care to finance. However, this progress has also given rise to a dark side, notably cybercrime and data breaches. These phenomena have evolved in tandem with technological advancements, and understanding their scope, causes, and consequences is crucial for formulating effective solutions.

Results

Increase in Cybercrime Activities

Research has revealed a sharp increase in cybercrime activities over the past decade. According to a report by the FBI's internet Crime Complaint Center (IC3), there is a 69% increase in reported cybercrime incidents between 2020 and 2022. This uptick can be attributed to several factors, including the widespread use of digital platforms for business and personal activities and the growing sophistication of cybercriminal techniques. Phishing, ransomware attacks, and identity theft are the most common forms of cybercrime.

Data Breaches and Their Consequences

Data breaches have become an alarming reality, with over 4.1 billion records exposed in 2020 alone, a 140% increase from the previous year. These breaches often target sensitive personal information such as credit card details, social security numbers, and health records. The consequences are far-reaching: individuals suffer from identity theft, whereas companies face financial losses, reputational damage, and legal consequences. The breach of a major health insurer in 2020 resulted in the exposure of millions of patients' personal health information, highlighting the vulnerability of the healthcare sector.

Emerging Threats

With the rise of emerging technologies such as artificial intelligence (AI), the IoT, and 5G networks, cybercriminals have exploited new vulnerabilities. IoT devices, which often lack sufficient security protocols, have become prime targets for attacks. Moreover, the adoption of AI in cybercrime has enabled attackers to launch more sophisticated and automated attacks, making detection and prevention significantly more difficult.

Discussion

The rise of cybercrime and data breaches is not merely a byproduct of technological advancements but rather an inherent flaw in how these technologies have been adopted and managed. The increasing sophistication of cybercriminals presents a significant challenge to both the public and private sectors in terms of securing digital spaces. One of the main reasons for this surge is insufficient cybersecurity measures for businesses and individuals. Many small- and medium-sized enterprises (SMEs) struggle to afford robust security systems, leaving them vulnerable to attacks.

Another key factor contributing to this surge is the lack of global coordination for combating cybercrime. Cybercriminals often operate in jurisdictions with lax laws, making it difficult for authorities to track and prosecute offenders. Additionally, the anonymity provided by the internet, particularly through tools such as Virtual Private Networks (VPNs) and the Dark Web, has enabled criminals to operate with relative impunity.

Furthermore, as more personal data is stored online, the stakes for data breaches continue to increase. With increasing amounts of data being shared across multiple platforms, often without clear consent or robust security measures, the potential for large-scale data theft is significantly higher. In many cases,

companies that suffer breaches fail to inform the affected parties on time, exacerbating the long-term impact on victims.

The emerging role of AI and machine learning in cybercrime is of particular concern. Attackers are increasingly using AI to automate attacks such as phishing, which makes it harder for traditional security measures to detect and prevent them. AI can also be used to analyze large amounts of stolen data, potentially uncovering even more sensitive information that can be used for further exploitation.

While technology offers many solutions to enhance cybersecurity, such as advanced encryption methods, AI-driven threat detection, and blockchain-based solutions, it is also clear that increasing reliance on digital systems demands a holistic approach to security. Governments, businesses, and individuals must collaborate to ensure better safeguards are put in place, including stricter data protection regulations, rigorous enforcement of existing cybersecurity laws, and enhanced public awareness campaigns.

Addressing the rise of cybercrime and data breaches requires a multifaceted approach that encompasses technological, legal, and societal changes. Although technology can be both the cause and the solution, we need more than just advanced tools to combat this issue. Stronger regulatory frameworks, proactive cyber-hygiene practices, and international cooperation are necessary to mitigate the risks and protect users from the growing threat posed by cybercrime.

CONCLUSION AND RECOMMENDATIONS

The dark side of technology is undoubtedly the rise of cybercrime and data breaches. As stratagems are becoming much more brazen and insidious than before, there is an urgent need for comprehensive approaches to counter emerging risks. Section 1 outlines the structure of this study. It further investigates analytical approaches to addressing new and emerging cyber risks, explores network security, application security, and incident response, and presents a thematic analysis and synthesis of research on the impact of COVID-19 on global cybersecurity risk discourse.

There are several key takeaways that resulted from this investigation. At the FBI, IC3 observed a steady increase in the volume of complaints, particularly those related to the COVID-19 pandemic. An overwhelming category of victims is those over the age of 60 years. Small businesses must work together with community colleges, SBA, FBI, and private sector partners, sharing the same knowledge pool and providing community awareness to prevent best practices on cyber and scam crime to reduce the risk of becoming victims of cybercrime and breaches. With an online market culture, any e-commerce threats we can imagine are likely to occur. Recommended for all e-commerce actors is enhanced cybersecurity training, awareness programs, safety features, investing in technology, and encouraging the use of safer payment methods.

REFERENCES

1. Liu X, Ahmad SF, Anser MK, Ke J, Irshad M, Ul-Haq J, et al. Cyber security threats: a never-ending challenge for e-commerce. Front Psychol. 2022;13:927398. doi:10.3389/fpsyg.2022.927398
2. Hewana S. The representation of the use of social media for committing cyber-crimes in selected South African newspapers [Master's thesis]. Nelson Mandela Metropolitan University, Faculty of Arts; 2025.
3. Abdulai M. Determinants of fear of cybercrime victimisation: a study of credit/debit card fraud among students of the University of Saskatchewan [thesis]. Saskatoon (SK): University of Saskatchewan; 2016 May 20. Available from: https://harvest.usask.ca/items/4ea3c0f8-7448-4f44-a370-a0f6b071898e
4. Xiaolin ES. Cyber security: basics in fighting computer attacks and crimes. Computer. 2017; 7(3): 21–27.

5. McDaniel B. An in-depth look into cybercrime. Themis. 2018;6(1):10. doi:10.31979/THEMIS.2018.0610
6. Porcedda MG, Wall DS. Cascade and chain effects in big data cybercrime: lessons from the TalkTalk hack. 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Stockholm, Sweden. 2019. p. 443–452. doi:10.1109/EuroSPW.2019.00056
7. Parn EA, Edwards D. Cyber threats confronting the digital built environment: common data environment vulnerabilities and blockchain deterrence. Eng Constr Archit Manag. 2019;26(2):245–266. doi:10.1108/ECAM-03-2018-0101
8. Cannon JE. Strategies for improving data protection to reduce data loss from cyberattacks [doctoral dissertation]. Minneapolis (MN): Walden University; 2019. Available from: https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=8554&context=dissertations
9. Ertan A, Crossland G, Heath C, Denny D, Jensen R. Cyber security behaviour in organisations [preprint]. 2020. arXiv:2004.11768. doi:10.48550/arXiv.2004.11768.
10. Uchendu B, Nurse JRC, Bada M, Furnell S. Developing a cyber security culture: current practices and future needs. Comput Secur. 2021;109:102387. doi:10.1016/j.cose.2021.102387
11. Edwards M, Williams E, Peersman C, Rashid A. Characterising cybercriminals: a review [preprint]. 2022. arXiv:2202.07419. doi:10.48550/arXiv.2202.07419.
12. Peersman C, Williams E, Edwards M, Rashid A. Understanding motivations and characteristics of financially motivated cybercriminals [preprint]. 2022. arXiv:2203.08642. doi:10.48550/arXiv.2203.08642.
13. Akter S, Uddin MR, Sajib S, Lee WJT, Michael K, Hossain MA. Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Ann Oper Res. 2022;1–26. doi:10.1007/s10479-022-04844-8
14. Buil-Gil D, Trajtenberg N, Aebi MF. Measuring cybercrime and cyberdeviance in surveys. In: Graham RS, Humer SG, Lee CS, Nagy V, editors. The Routledge International Handbook of Online Deviance. London: Routledge; 2025. p. 44–72. doi:10.4324/9781003277675-4.
15. Ayofe AN, Oluwaseyifunmitan O. Approach to solving cybercrime and cybersecurity [preprint]. 2009. arXiv:0908.0099. doi:10.48550/arXiv.0908.0099.
16. Uwadia CO, Omogbadegun ZO, Fasina EP. Cybercrime pervasiveness, consequences, and sustainable counter strategies. J Comput Sci Its Appl. 2006;13(1):11–24.
17. Mills JL, Harclerode K. Privacy, mass intrusion and the modern data breach. Fla Law Rev. 2017;69(3):771–818. Available from: https://scholarship.law.ufl.edu/flr/vol69/iss3/3
18. De Villiers M. Enabling technologies of cyber crime: why lawyers need to understand it. SSRN Electron J. 2011;11:i. doi:10.2139/ssrn.1927080
19. Dilek S, Çakır H, Aydın M. Applications of artificial intelligence techniques to combating cyber crimes: a review [preprint]. 2015. arXiv:1502.03552. doi:10.48550/arXiv.1502.03552.
20. Barosy W. Successful operational cyber security strategies for small businesses [doctoral dissertation]. Minneapolis (MN): Walden University; 2019.
21. Balogun AM, Zhu SY. Privacy impacts of data encryption on the efficiency of digital forensics technology. Int J Adv Comput Sci Appl. 2013;4(5):36–40. doi:10.14569/IJACSA.2013.040506.
22. Rawal A, Khanna H, Kaur G. Cryptography: symmetric vs asymmetric encryption. J Embedded Syst Process. 2018;3(3):1–5.
23. Cervera García AC, Goussens A. Cybersecurity and use of ICT in the health sector. Aten Primaria. 2024;56(3):102854. doi:10.1016/j.aprim.2023.102854.
24. McMenemy D. Digital Ethics: a UKeiG White Paper. London: UKeiG; 2016. p. 1–27.
25. Inserra D. Cybersecurity beyond US borders: engaging allies and deterring aggressors in cyberspace. Washington (DC): Heritage Foundation; 2017.
26. Williams M, Axon L, Nurse JRC, Creese S. Future scenarios and challenges for security and privacy. Future scenarios and challenges for security and privacy. 2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI), Bologna, Italy. 2016. p. 1–6. doi:10.1109/RTSI.2016.7740625.

