China Petroleum Processing and Petrochemical Technology

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

STRATEGIES AND CHALLENGES IN COMBATING CYBERCRIME: A COMPREHENSIVE ANALYSIS OF CYBERSECURITY TECHNOLOGIES, LEGAL FRAMEWORKS, AND PREVENTATIVE MEASURES

Urvi Sharma

M.Tech (IT) Cyber Security, Indira Gandhi Delhi Technical University for Women, Kashmiri Gate, New Delhi

Abstract

In the digital age, cybercrime has emerged as a formidable challenge, evolving in complexity and scale. This research delves into the multifaceted nature of cybercrime, from its various types - ranging from financial frauds to attacks on personal privacy - to the profound impacts it has on economies, societies, and national security. With technological advancements, new vulnerabilities manifest, particularly in areas like the Internet of Things, augmented and virtual reality platforms, and the world of cryptocurrencies. Legal frameworks, both at national and international levels, are continually adapting to address these threats. The paper emphasizes the importance of proactive measures, such as public education and technological safeguards, while also highlighting the necessity for international cooperation to tackle cross-border cybercrimes effectively.

Keywords: *Cybercrime, Internet of Things, Augmented Reality, Cryptocurrencies, Legal Frameworks, Public Education, Cybersecurity, International Cooperation, Digital Vulnerabilities, Financial Frauds.*

1 INTRODUCTION

Cybercrime, at its core, encompasses a range of malicious activities conducted via digital means, often targeting computer systems, networks, and data. These can range from financial fraud, unauthorized data breaches, to the distribution of malicious software or malware (Johansen, Alison Grace, 2020). As technology has rapidly evolved and become integral to personal, corporate, and governmental operations, so has the sophistication and scale of cybercrimes. The scope is vast, including crimes like identity theft, cyberbullying, espionage, and even cyberterrorism. Given the borderless nature of the internet, cybercrimes often transcend national jurisdictions, making their mitigation and prosecution particularly challenging (Security Bill - FINAL with Amendments 12th Sept 2019).

The Pervasiveness of Cybercrime in Today's Digital Landscape: Today's digital age, marked by the ubiquity of internet-connected devices, the rise of e-commerce, and the increasing digitization of personal information, has inadvertently provided a fertile ground for cybercriminals.

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

The threats are not just limited to individuals or businesses. Critical infrastructures, like power grids or water supply systems, which increasingly rely on digital systems, are also at risk, underscoring the potential large-scale implications of cyberattacks (Byres, Eric, and Justin Lowe, 2004). With the expanding Internet of Things (IoT), where everyday objects from fridges to cars are connected to the internet, the potential points of vulnerability multiply (Abomhara, Mohamed, and G. M. Kien, 2015). As cyber threats become more prevalent, understanding their nature, implications, and devising effective legal and technical responses become paramount.

2. LITERATURE REVIEW

Various harmful actions carried out via digital methods, often aimed against computer systems, networks, and data, constitute cybercrime. Financial fraud, unauthorised data breaches, and the propagation of dangerous software or malware are all examples of what might be considered as such (Johansen, Alison Grace, 2020). Cybercrimes have grown in complexity and scope in tandem with the fast development and pervasiveness of technology in all spheres of life. A wide range of offences are included, including cyberterrorism, cyberbullying, espionage, and identity theft. The internet's global reach makes it difficult to contain and punish cybercrime, which poses unique challenges for law enforcement (Security Bill - FINAL with Amendments 12th Sept 2019).

Types of Cybercrimes

- **Financial Frauds: Phishing, Skimming, and Cryptocurrency Scams:** Financial frauds represent one of the most lucrative avenues for cybercriminals. Phishing attacks, where unsuspecting users are tricked into revealing sensitive information through deceptive emails or websites, remain prevalent (Johansen, Alison Grace, 2020). Skimming, on the other hand, involves capturing card details through compromised point-of-sale terminals. The rise of cryptocurrencies has also ushered in a new wave of scams, with attackers exploiting the digital nature and relative anonymity of these currencies to defraud victims.
- **Attacks on Privacy: Data Breaches, Identity Theft, and Doxxing:** Privacy attacks have become increasingly sophisticated. Data breaches involve unauthorized access to databases, leaking vast amounts of personal and financial data. Such breaches not only have financial implications but also erode trust in digital systems. Identity theft extends beyond financial ramifications, affecting victims' personal and professional lives. Doxxing, the malicious act of publicly revealing private information about an individual without their consent, can have dire personal and psychological consequences for the victims.
- **Content-related Offenses: Cyberbullying, Revenge Porn, and Hate Speech:** The internet, while fostering connections, has also become a platform for various content-related offenses. Cyberbullying, targeting individuals with threats, humiliation, or harassment online, has seen a significant surge, especially among younger populations. Revenge porn, the unauthorized distribution of intimate images, and hate speech,

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

promoting violence or prejudice against particular groups, further exemplify the darker side of online interactions (Razzaq, Abdul, et al., 2013).

- **Malware, Ransomware, and Advanced Persistent Threats:** Malware, short for malicious software, represents programs designed to infiltrate and damage computer systems. Ransomware, a subset of malware, encrypts victims' data, demanding a ransom for its release. Advanced Persistent Threats (APTs) signify sophisticated, prolonged cyber-attacks aimed at stealing data from organizations, often orchestrated by well-funded entities or state actors (Ten, Chee-Wooi, Chen-Ching Liu, & Govindarasu Manimaran, 2008).

Impact of Cybercrime

- **Economic Implications: Financial Losses and Market Trust:** Cybercrimes carry severe economic consequences. Beyond the immediate financial losses incurred by individuals or organizations due to fraud or ransom demands, there's a cascading effect on market trust. Businesses, especially those in the e-commerce sector, suffer reputational damage after data breaches, leading to lost business opportunities and decreased consumer confidence. The costs of mitigating cyberattacks, legal fees, and potential regulatory fines further strain financial resources. Moreover, the global economy bears the brunt, with billions lost annually due to cybercrimes (Rowe, Dale C., Barry M. Lunt, & Joseph J. Ekstrom, 2011).
- **Social Implications: Privacy Concerns and Psychological Effects:** The social implications of cybercrime are vast and multi-faceted. Privacy breaches lead to a climate of distrust in digital platforms, impeding the digital progression and causing hesitancy in adopting new technologies. Victims of cyberbullying, doxxing, or revenge porn often undergo severe psychological distress, leading to issues like depression, anxiety, and, in extreme cases, even suicide. The ubiquitous nature of the internet means that such crimes can have prolonged effects, with victims' information or malicious content remaining accessible and causing recurring trauma (Razzaq, Abdul, et al., 2013).
- **Security Implications: National Security and Infrastructure Threats:** Cybercrimes aren't limited to individual or corporate targets. Increasingly, nation-states or affiliated actors deploy cyber-attacks to further political, ideological, or military goals. These can range from hacking government databases, influencing elections, or even disabling critical infrastructure such as power grids or transportation systems. Such attacks can cripple a nation's functionality, leading to widespread chaos and potentially endangering lives. The interconnected nature of today's world means that cyber warfare can have ramifications far beyond the immediate target, affecting global geopolitics and security (Al-Mohannadi, Hamad, et al., 2016).

Legal Frameworks Addressing Cybercrime

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

- **National Laws and Regulations: A Comparative Analysis:** Different countries approach cybercrime with varying levels of stringency and focus. For instance, countries like the United States have laws like the Computer Fraud and Abuse Act (CFAA) that criminalizes unauthorized access to computer systems. The European Union has introduced the General Data Protection Regulation (GDPR), emphasizing data protection and privacy for all individuals within the EU and the European Economic Area (EEA). In Asia, countries like Singapore have instituted the Computer Misuse and Cybersecurity Act, targeting unauthorized computer use. Meanwhile, nations like Sri Lanka have introduced specific cyber security bills, such as the one from September 12, 2019, to address the evolving landscape of cyber threats (Security Bill - FINAL with Amendments 12th Sept 2019, 2019).
- **International Collaborations and Treaties: Budapest Convention and Others:** Given its borderless nature, cybercrime demands international cooperation. The Council of Europe's Budapest Convention, also known as the Convention on Cybercrime, stands out as a pivotal international treaty offering a collective approach to combating cybercrime. This convention presents guidelines for countries developing comprehensive national legislation against cybercrime and fosters international cooperation. Beyond the Budapest Convention, other multilateral agreements and collaborations facilitate data sharing, investigative assistance, and capacity-building measures to bolster global resilience against cyber threats (Al-Mohannadi et al., 2016).

Challenges in Combatting Cybercrime

- **Jurisdictional Issues: Tracking Cross-border Offenses:** One of the primary hurdles in addressing cybercrime lies in its inherently global nature. Offenders can initiate attacks from one country and target victims in another, making traditional jurisdictional approaches ineffective. For instance, a hacker based in Eastern Europe can compromise a server in Asia to target a corporation in North America. This geographical dispersion not only complicates investigative procedures but also raises legal questions about where a crime has occurred and under whose jurisdiction it falls. Such complexities often impede swift legal actions, as international cooperation becomes paramount yet remains challenging (Al-Mohannadi et al., 2016).
- **Technical Challenges: Encryption, Dark Web, and Rapid Technological Advancements:** As technology evolves, so do the methods of cybercriminals. Advanced encryption techniques can protect users' privacy, but they can also shield criminal activities, making it challenging for law enforcement agencies to intercept and decipher malicious communications (Johansen, 2020). Moreover, the dark web provides a platform for various illicit activities, from selling stolen data to trading in illegal goods, further complicating monitoring efforts (Razzaq et al., 2013). The pace of technological

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

advancements often outstrips the speed at which legal frameworks can adapt, leaving gaps that cybercriminals exploit.

- **Legal Challenges: Balancing Privacy Rights and Law Enforcement Needs:** The legal realm grapples with the delicate balance between individual privacy rights and the necessities of law enforcement. While surveillance and data collection can aid in preempting and investigating cybercrimes, they also pose risks to personal privacy and can be prone to misuse. Laws like the GDPR in the European Union underscore the importance of data protection and user consent, but they can also limit the extent to which data can be accessed for investigative purposes (Security Bill - FINAL with Amendments 12th Sept 2019, 2019). Striking the right balance ensures that while cybercrimes are effectively addressed, individual rights aren't compromised.

Role of Technology in Preventing and Detecting Cybercrime

- **Advanced Threat Detection and AI-driven Security Measures:** Emerging technologies, especially Artificial Intelligence (AI) and Machine Learning (ML), play pivotal roles in detecting and mitigating cyber threats. AI-driven security tools can analyze vast amounts of data at unprecedented speeds, identifying patterns and anomalies that may suggest malicious activities (Moti Zwilling et al., 2020). These tools can predict potential threats and automate responses, thereby enhancing the proactive and reactive capabilities of security systems. Automated threat detection can filter out known malware and flag suspicious behaviors, ensuring quicker response times and reducing the reliance on human intervention.
- **Blockchain and Decentralized Systems for Enhanced Security:** Blockchain technology, originally developed for cryptocurrencies, offers immense potential for cybersecurity. Its decentralized nature ensures that data isn't stored in a single location, making it resistant to common cyber threats like Distributed Denial of Service (DDoS) attacks. Additionally, once data is entered into a blockchain, it becomes immutable, which prevents data tampering. The transparent and traceable nature of blockchain transactions also aids in tracking malicious activities and their origins (Byres and Lowe, 2004). As industries beyond finance begin to recognize its potential, the application of blockchain in ensuring data integrity and security is rapidly expanding.
- **User Education and Awareness Programs:** While technology offers robust tools for security, the human element remains a crucial aspect of cybersecurity. Many cyber incidents result from human error or oversight. As such, educating users becomes paramount. Awareness programs, workshops, and training sessions can equip users with knowledge about potential threats like phishing emails, unsafe websites, and the importance of strong, unique passwords. By creating a more informed digital community, the risks associated with human errors can be significantly reduced (Shaw RS et al., 2009).

3. METHODOLOGY

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

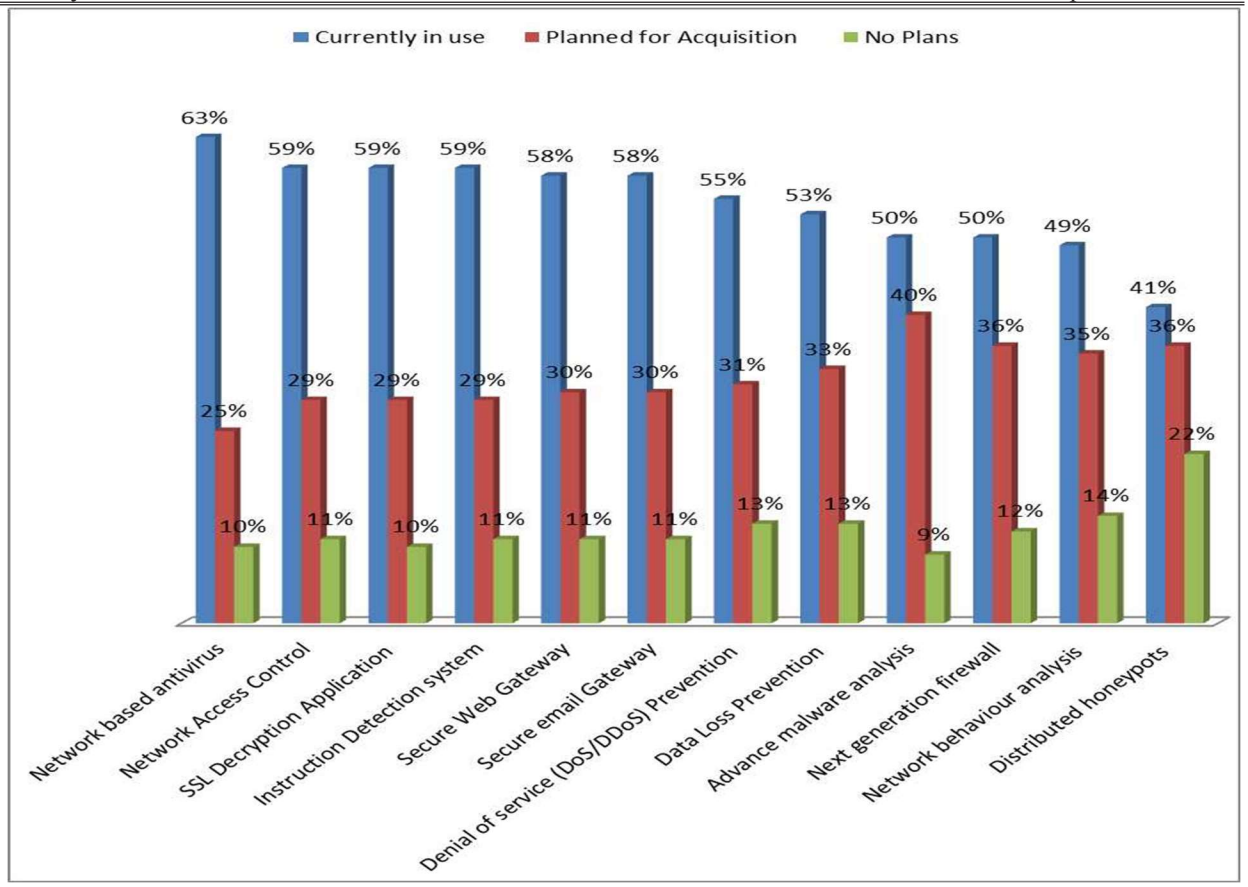
The methodology employed in the analysis of cybercrime and its multifaceted impacts is comprehensive, encompassing data collection, categorization, and evaluation across various dimensions of cyber threats. This involves gathering and analyzing data from diverse sources, including industry reports, government documents, and international conventions, to understand the spectrum of cybercrimes, from financial frauds to privacy attacks and advanced persistent threats. A significant aspect of the methodology is the industry-specific impact analysis, where data from different sectors such as healthcare, finance, and education is scrutinized to assess the unique vulnerabilities and economic impacts of cyber incidents in each field. Furthermore, the research delves into the legal frameworks at national and international levels, comparing various laws and regulations, including the Budapest Convention, to evaluate their effectiveness against the evolving landscape of cybercrime. Technological countermeasures, such as AI-driven security tools and blockchain technology, are also critically assessed for their role in enhancing cyber defense. Importantly, the methodology recognizes the human factor in cybersecurity, analyzing the impact of user education and awareness programs in mitigating human error-related vulnerabilities. Finally, the research addresses the challenges in combatting cybercrime, including jurisdictional and technical difficulties, and legal complexities, setting the stage for future research directions in developing more robust security architectures and enhancing situational awareness in the digital realm. This multifaceted methodological approach provides a holistic understanding of the current state of cybercrime, its impacts, and the concerted global efforts required to mitigate its risks.

4. PERFORMANCE ANALYSIS OF DIFFERENT NETWORK SECURITY TECHNOLOGIES

This paper proposes a methodology that classifies network protection technologies, web apps and malicious programmes, vulnerabilities with the highest increased danger, this year's computer security spending targets, and attacks according to threat type, targeted field, purpose, effect, and incident classifications. The taxonomies have been updated to reflect this new information. There will be easy-to-understand explanations of each stage of the assault.

Figure 1: Network Security technologies in use and planned for acquisition.

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

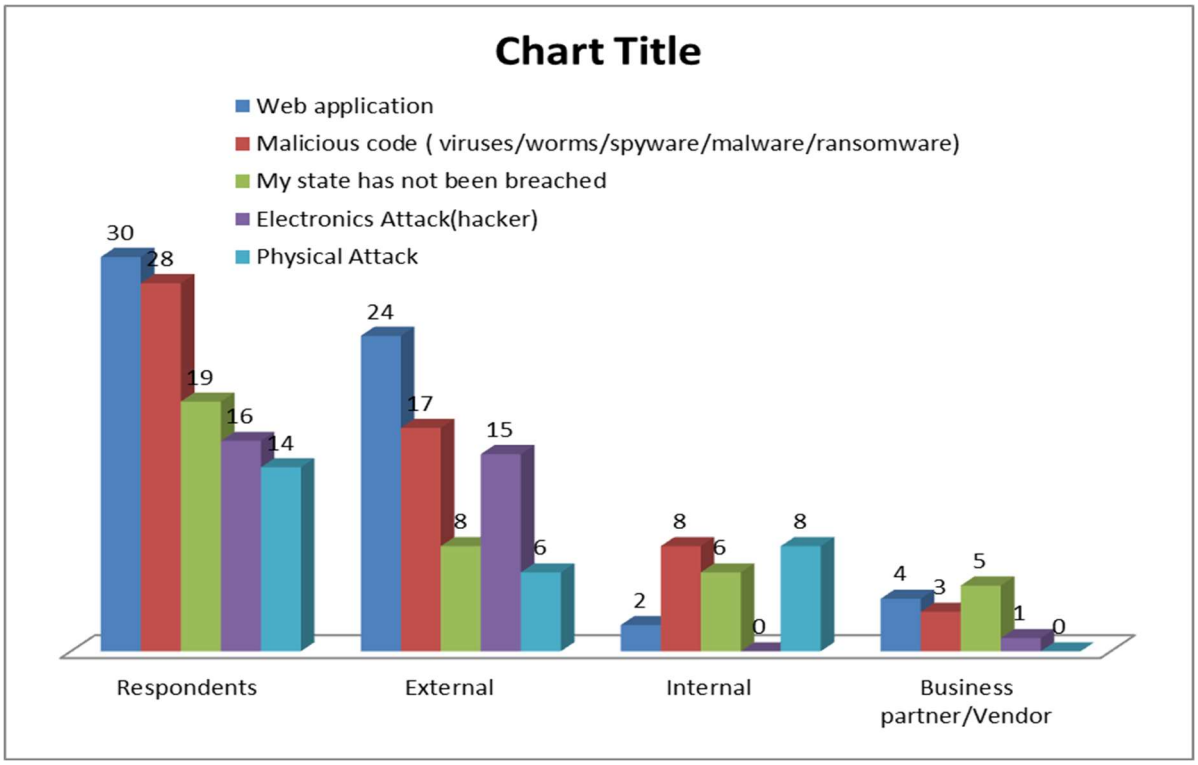


Source: -2020 Deloitte-NASCIO Cyber security Study

Companies and organisations from all around the globe are boosting their investment in order to accommodate these and other advancements. Although there are significant differences across economies and sector sizes, predictions of data security expenditure imply that there are considerable disparities between them.

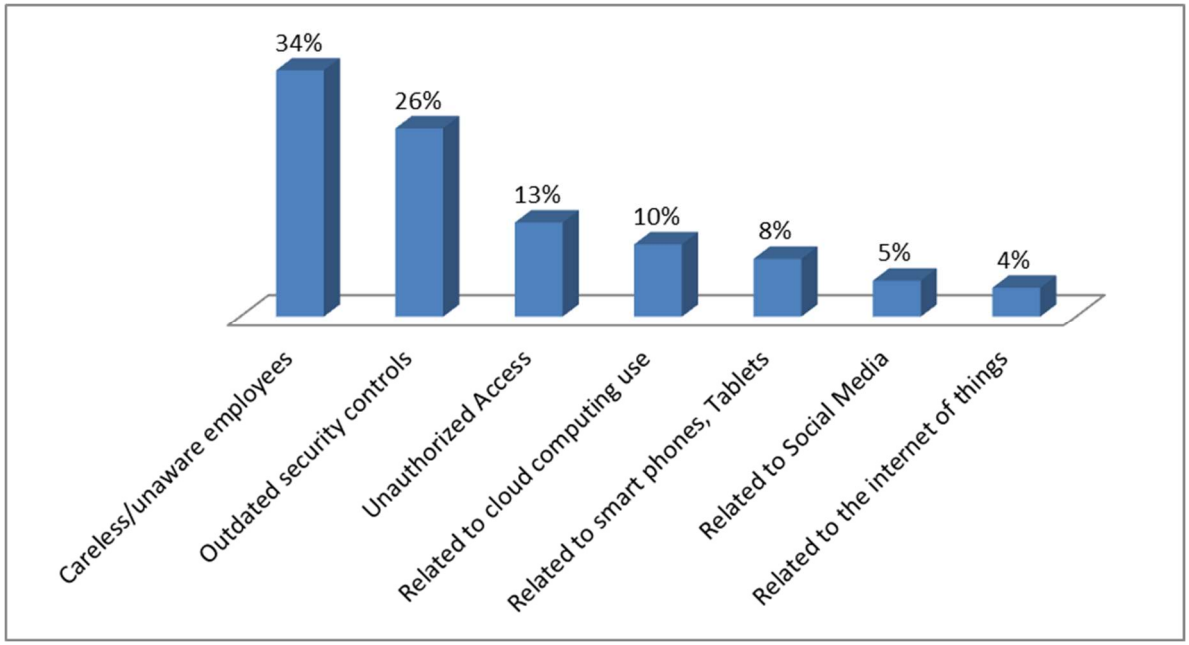
Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

Figure 2 Web applications and malicious code are the leading sources of security breaches.



Source: -2020 Deloitte-NASCIO Cyber security Study

Figure 3 Vulnerabilities with the most increased risk exposure over the past 12 months.



Source: -2020 Deloitte-NASCIO Cyber security Study

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

Table:1 Global Information Security Survey 2022-2023

Valuable information to cyber criminals	Targeted attack	Cyber Threats to Organizations	Cyber Threats
Customer information	17%	Phishing	20%
Financial information	12%	Malware	20%
Strategic plans	12%	Cyber-attacks (to disrupt)	13%
Board member information	11%	Cyber-attacks (to steal money)	12%
Customer passwords	11%	Fraud	10%
R&D Information	9%	Cyber-attacks (to steal IP)	8%
M&A Information	8%	Spam	6%
Intellectual property	6%	Inter Attacks	5%
Non-Patented IP	5%	Natural Disasters	2%
Supplier Information	5%	Espionage	2%

The foundation of cyber security is the defence against unauthorised and/or unintentional access to computers, networks, services, and data. In recent times, cyber security has become a very important topic due to the fact that governments, organisations, and people are responsible for collecting, processing, and archiving massive amounts of sensitive information, and then distributing this information across networks. Over the course of the last several years, data misuse has become nearly commonplace. Over the course of the previous several years, the market for advanced technology and defensive solutions has increased as a result of high-profile instances of cyber hacking. Companies all around the world are becoming more aware of the impending danger, which results in a greater allocation of resources to businesses that contribute to the mitigation of such dangers.

Despite the fact that some organisations are susceptible to cyber risks as a result of specific mishaps (in the year 2020, almost 82% of accidents that occurred in the hospitality industry were caused by point-of-sale systems), this table demonstrates that in many ways, all industries are susceptible to cybercrime. As a consequence of this, considering the level of complexity of cyber threats, there has been an increasing need for cyber security services.

Table 2: Industries affected by different types of incidents

Incidents by industry	Crim e ware	Cyber Espiona ge	Denial of service	Energy thing else	Stole n assets	Mics errors	Card skimm ers	Privile ge misuse	Poin t of sale	Web applica tions

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

Accommodation	5.65	1.88	0.27%	3.49%	1.08%	0.54%	1.61%	0.27%	82.26%	2.96%
Education	6.51	2.40	51.71	16.44	3.42	5.48	0.00	4.11	0.00	9.93
Financial	8.18%	3.51%	56.09%	9.85%	2.65%	3.67%	8.18%	1.50%	0.33%	6.01%
Healthcare	20.51	18.38	0.13	8.39	12.78	24.10	0.67	3.20	0.13	11.72
Information	1.87	0.16	19.06	2.66	0.10	1.12	0.00%	0.13	0.07	74.83
Manufacturing	52.89	4.10	13.78	7.26	2.79	0.56	0.19	15.27	0.00	3.17
Professional	45.59	5.15	19.12	7.54	3.13	5.51	0.00	7.54	0.18	6.25
Public	26.27	45.24	3.08	0.30	16.36	7.78	0.00	0.53	0.00	0.43
Retail	8.20%	3.47	26.81	3.79	2.21	3.47	25.55	0.00	3.47	23.03

Investors may get exposure to the cyber security business via the L&G Cyber Protection programme, which is one method to do so. What is under the surface is the cyber security. It is vital to completely identify both the growth determinants of cyber security and the outlook of the market in order to have a better understanding of the variables that contribute to the need of cyber security from an economic perspective. An examination of the variables that contribute to the growth of cyber security and the market forecast will be shown in the ensuing study. Following this, an explanation of the ways in which the aforementioned cyber security index is able to capture these positive developments in the area of cyber security will be provided.

Table 3 Priorities for cyber security investment this year and compared to last year.

Computing security	**High Priority**		**Medium Priority**		**Low Priority**	
	Current Year	Previous Year	Current Year	Previous Year	Current Year	Previous Year
Cloud computing	52%	57%	37%	37%	11%	06%
Cyber security analysis	38%	52%	50%	43%	11%	5%
Mobile computing	33%	35%	52%	58%	16%	7%
Internet of things	25%	29%	27%	61%	48%	9%
Robotics process automation	18%	31%	45%	58%	37%	11%
Machine learning	16%	27%	48%	61%	36%	11%
Artificial intelligence	15%	26%	43%	63%	39%	11%

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

Bio-matrices	15%	15%	44%	72%	41%	13%
Blockchain	14%	15%	37%	69%	48%	15%

5. CONCUSION AND FUTURE WORK

A few simple steps to ensure the security and privacy of online interactions. Enable the antivirus programme. It seems that antivirus software is normally pre-installed on most computers. Fortunately, there are many of free and paid antimalware services to choose from if it isn't enough. Modern antimalware software often use a two-pronged approach to identify and remove ransomware. To begin, there is the standard device search, which involves running an antivirus scan over every file on the computer in an effort to detect, encrypt, and remove any harmful software. In the second, known as real-time monitoring, all installed files and processes are checked and recognised accurately as they show up on the device.Virtual private networks, or VPNs, encrypt all data sent over the internet and redirect it to a destination of the user's choosing via a distant server. In most cases, commercial VPNs are subscription services that charge users to use the service via a mobile app. They have two important outcomes. The first is an encrypted tunnel that all data passes through before it reaches the VPN registry. This prevents hackers and ISPs from monitoring any and all online traffic, which is the ultimate goal of r traffic. The second is that an IP address—a unique number that may be used to identify between devices and locations—is disguised behind the VPN host address.The online activities might be more discreet in this way. It is difficult to trace activity back to a particular user since most commercial VPNs group a large number of users together under a single IP address.Web browsers are windows into the world wide web, which can accomplish many things but is also vulnerable to many risks and weaknesses; one purpose for a virtual private network (VPN) is to unblock geo-locked material that is only accessible from certain countries, such as US Netflix or Hulu. Over the last two decades, cyber risks and cybersecurity have grown at an exponential rate, thanks to technological advancements. However, despite this, the majority of companies have not progressed and are still relying on cyber defence. These fifth-generation assaults are known as big attacks because they are similar to second- or third-generation attacks in magnitude and speed, but they occur after the fifth-generation attacks have emerged. The conventional, static security measures that are centred on inspection and used by the majority of organisations today would be readily evaded by this sophisticated attacker. When it comes to protecting their networks, cloud, and mobile devices against the latest attacks, organisations should also implement a fifth-generation security architecture. Finally, people and businesses should learn more about cyberattacks, their consequences, and how to protect themselves. Before using the app, everyone should weigh the benefits and drawbacks, look out for security breaches, and take measures to safeguard their data. In order to protect the assets of online platforms, including aws, smartphones, and communications infrastructure, researchers will focus on developing a fifth-generation security architecture in the future.

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

To shed light on some of these commonalities, this introduction is designed. Ultimately, it hopes that the reader will take away two important ideas. The cyber security problem will never be permanently resolved. Although they may have limited scope and durability, solutions to the problem are technically sound and so equally non-technical. Think about cyber security threats; it's a conservative objective and a creative requirement. There has to be a rethinking and rebirth of organised tactics to deal with resistant vulnerability treatments since the exponential growth of technology and infrastructure is a major cause and driver of cyber security challenges. Finally, the defence society's information and communication technology (ICT) system and architecture are responding to the ever-expanding development and growth by placing a priority on threat reduction, recovery, and eradication. Ultimately, for cyber security models to succeed in eradicating conflicting goals and interests, situational awareness must be improved in every scenario and at every level.

REFERENCES

1. *Security Bill - FINAL with Amendments 12th Sept 2019.pdf, <https://www.cert.gov.lk/Downloads/Cyber%20Security%20Bill%20-%20FINAL%20with%20Ammedments%2012th%20Sept%202019.pdf> Accessed 15th March 2021*
2. *Johansen, Alison Grace, What is a computer Virus, (Norton Life lock, July 23rd 2020) <https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html> Accessed 15th March 2021*
3. *Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin & Hamdullah Nejat Basim (2020): Cyber Security Awareness, Knowledge and Behaviour: A Comparative Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1712269 <https://www.researchgate.net/profile/Fatih-Cetin-3/publication/339273589_Cyber_Security_Awareness_Knowledge_and_Behavior_A_Compa rative_Study/links/5e46ef2ba6fdccd965a5c9be/Cyber-Security-Awareness-Knowledge-and-*
4. *Behavior-A-Comparative-Study.pdf> Accessed 17th March 2021*
5. *Shaw RS, Chen CC, Harris AL, Huang HJ. The impact of information richness on information security awareness training effectiveness. Comput Educ. 2009; 52(1):92–100.*
6. *Razzaq, Abdul, et al. "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. "Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013.*
7. *Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." Proceedings of the VDE Kongress. Vol. 116. 2004.*
8. *"Common Cyber Attacks: Reducing The Impact Gov.uk" https://www.gov.uk/...data/.../Common_Cyber_Attacks-Reducing_The_Impact.pd*

Catalyst Research Volume 23, Issue 2, December 2023 Pp. 4630-4642

9. *"CYBERSECURITY: CHALLENGES FROM A SYSTEMS, COMPLEXITY,KNOWLEDGE MANAGEMENT AND BUSINESS INTELLIGENCE PERSPECTIVE" Issues in Information Systems Volume 16, Issue III, pp. 191-198, 2015*
10. *"Cyber security: risks, vulnerabilities and countermeasures to prevent social Engineering attacks" International Journal of Advanced Computer Research, Vol 6(23) ISSN (Print): 2249-7277 ISSN (Online): 2277-7970 http://dx.doi.org/10.19101/IJACR.2016.623006*
11. *Ahmad, Ateeq. "Type of Security Threats and It's Prevention." Int. J. Computer Technology & Applications, ISSN (2012): 2229-6093.*
12. *Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran. "Vulnerability assessment of cyber security for SCADA systems." IEEE Transactions on Power Systems 23.4 (2008): 1836-1846.*
13. *"Cyber Crime-Its Types, Analysis and Prevention Techniques", Volume 6, Issue 5, May 2016 ISSN: 2277 128X www.ijarcsse.com*
14. *"A Review of types of Security Attacks and Malicious Software in Network Security" Volume 4, 10. Abomhara, Mohamed, and G. M. Kien. "Cyber security and the internet of things: vulnerabilities, threats, intruders and attacks." Journal of Cyber Security 4 (2015): 65-88.*
15. *"Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users" International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:9, No:3, 2015*
16. *"Detection and Prevention of Passive Attacks in Network Security" ISSN: 2319-5967 ISO 9001:2008 Certified International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 6, November 2013*
17. *Al-Mohannadi, Hamad, et al. "Cyber-Attack Modeling Analysis Techniques: An Overview." Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on. IEEE, 2016.*
18. *"Internet Security Threat Report Internet Report "VOLUME 21, APRIL 2016https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf*
19. *Rowe, Dale C., Barry M. Lunt, and Joseph J. Ekstrom. "The role of cyber-security in information technology education." Proceedings of the 2011 conference on Information technology education.ACM, 2011.*