WWW.IJRPR.COM

**International Journal of Research Publication and Reviews**

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

# The Digital Battlefield: Navigating the New Age of Cyber Warfare

***Shivam Patel[1], Kiran R Dodiya[2], Akash Khunt[3], Divya Patel[4], Prof. (Dr.) Nikunj Brahmbhatt[5], Sanjay Sharma[6], Dharmesh Vandra[7]***

[1.]M.sc Cyber Security NSIT-IFSCS, Jetalpur, Ahmedabad (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India(shivampatel9051@gmail.com)

[2.] Assistant Professor & Program Co-ordinator of DFIS (Cyber Security & Digital Forensics) NSIT-IFSCS Jetalpur, Ahmedabad (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India. (kirandodiya01@gmail.com)

[3.]Assistant Professor & Program Co-ordinator of Cyber Security (Cyber Security & Digital Forensics) NSIT-IFSCS Jetalpur, Ahmedabad (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India. (akpatel950@gmail.com)

[4.]Assistant Professor & Course Co-ordinator of DFIS (Cyber Security & Digital Forensics) NSIT-IFSCS, Jetalpur, Ahmedabad (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India. (pateldivyaa17@gmail.com)

[5.]Principal (NSIT-IFSCS), Jetalpur, Ahmedabad. (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India(principal@nsit.org.in)

[6.]Campus Director, NSIT-IFSCS), Jetalpur, Ahmedabad (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India(campusdirector@nsit.org.in)

[7.]Vice President, (NSIT-IFSCS), Jetalpur, Ahmedabad. (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India. (vicepresident@nsit.org.in)

**ABSTRACT:**

The cyber-attack has matured into one of the most potent threats facing the world regarding security, economy, and individual pockets in this fast-changing digital landscape. While the actual spurt in ransomware, phishing, and DDoS attacks has made way for more sophisticated blackmails like supply chain attacks. The review paper tries to understand recent cyber-attack trends, mainly focusing on strategies adopted by attackers, the widespread impacts such incidents create, and changing defences to reduce such threats. Cybercriminals have mastered techniques of cybercrime, exploiting emergent technologies like artificial intelligence, machine learning, and blockchain in the last ten years to perfect and scale attacks. Modern cyber-attacks have depicted how issues such as giant corporations and critical infrastructures, to mention a few, may result in extreme destruction in terms of finance, reputation, and operations. The issues led to increased cybersecurity factors that forced organisations into multi-layered defence mechanisms, zero-trust architecture, advanced threat detection systems, and regular cybersecurity audits. Then, it discusses the geopolitical impacts of cyber warfare: firstly, a surge in attacks on critical infrastructures at the nation-state level and, secondly, the use of cyberspace for strategic purposes. It also requires new regulations and guidelines from governments and cybersecurity bodies about increasing cyber resilience. However, the dynamic nature of such a threat landscape means such issues are continually evolving, so defence innovation is also required across sectors. This paper elucidates recent cyber-attack practices and the far-reaching consequences that must be met by understanding the response towards modern cyber threats. In dealing with the risks of cyber-attacks found more often today within the interdependent world, roles of global cooperation, proactive defence strategies, and robust incident response frameworks become indispensable.

**Keywords***:* Ransomware, Phishing, DDoS, Cybercriminals, Zero-trust Architecture, Cyber resilience.

## 1. Introduction

This is the first generation to experience unprecedented technological change in how individuals, businesses, and governments engage with and rely upon digital infrastructure. But this unparalleled shift into a connected world has led to a new wave of vulnerabilities that manifest individually and collectively. Cyber-attacks increase in number, scope, and complexity and threaten global security, economic stability, and individual rights today. Now that the systems are operated very deep within the critical infrastructure and our daily lives, the consequences of cyber threats exponentially grow. From an isolated and simple matter, this challenge has blossomed into a multifaceted issue that affects every single segment of society. Cyber-attacks are viewed as harmful, malicious attempts intending to penetrate information systems to commit data theft or alteration or deletion of data, demand money, or disrupt critical operations. Undoubtedly, the last decade has seen a crucial rise in cyber-attacks. Hackers and cybercriminals now use very advanced techniques to undertake these cyber-attacks. Industries have been transformed digitally, and remote work has notably risen, especially since the COVID-19 pandemic, which worsened things and even exposed organisations and individuals to more excellent threat effects than ever before. Major cyber-attack vectors include ransomware, data breaches, phishing campaigns, Distributed Denial of Service attacks, and many more. Recently, supply chain attacks have also

gained mainstream popularity. In this attack, the ransomware hackers encrypt the sensitive data and request cryptocurrency as ransom to decrypt the information. Hence, such high-profile breaches as the Colonial Pipeline in the United States and the WannaCry ransomware attack have redefined the far-reaching impacts of just one breach into critical infrastructure affecting millions. Another technique is phishing, which began much further back but has become sophisticated in using social engineering ploys to trick people into disclosing sensitive information. Nation-state-sponsored attacks have gained momentum recently as nations use cyber espionage and sabotage for strategic geopolitical advantages. The nation-states increasingly rely on cyber operations for espionage, intellectual property theft, and antagonistic political and economic stability disruption. That fact has catapulted tensions across global powers, making cyber warfare a more significant aspect of modern geopolitical conflict. Collective efforts by governments, organisations, and individuals will be required to solve the prevalence of cyber threats. Cybersecurity measures must keep pace with this ever-changing threat landscape. Now, firewalls and anti-virus software are not enough. Modern companies have a way of taking a much more holistic approach to security: zero-trust architecture, multi-factor authentication, AI-driven threat detection, real-time monitoring of network activities, and much more. According to regulatory requirements, many jurisdictions have introduced new frameworks to strengthen cyber resilience. Some of the brightest initiatives developed to evolve security standards include the European Union's General Data Protection Regulation and the United States' Cybersecurity and Infrastructure Security Agency. This review paper tries to analyse current cyber-attack trends, assess the far-reaching impacts such incidents have, and discuss strategies that governments, organisations, and individuals can take to step up and respond to the growing threats. Understanding the tactics used by cybercriminals and the cascading effects of major breaches can help prepare and build a more secure digital environment.

## 2. Related Work

A paper titled "**A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security**" reviews methods for detecting, protecting against, and analysing cyber-attacks' impact on innovative grid systems, mainly focusing on wind farms, PV systems, and communication channels. Key findings highlight using AI, blockchain, and cryptographic algorithms for securing communications. FDIA is identified as a significant concern, with machine learning models providing high detection accuracy. Cryptographic methods like elliptic curve encryption and blockchain enhance electricity trading and data protection security. Future directions call for developing decentralised defence systems, dynamic watermarking, and lightweight authentication schemes to address cyber threats in renewable energy and IoT-based intelligent grids. Paper titled "**A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions** "This review paper presents a detailed examination of cyber security challenges and solutions based on recent technological advancements. It divides the topic into three key sections: cyber security fundamentals, threats and attacks, and network security by layers. The review highlights the growing complexity of cyber-attacks due to the increased use of internet services and vulnerabilities in systems, software, and protocols. Common threats such as malware, cryptographic attacks, advanced persistent threats (APTs) are discussed, along with network-layer-specific attacks. The paper emphasises technical solutions, including cryptography, AI, blockchain, machine learning, and nontechnical approaches like policy, risk management, and user training. Despite advancements in detection technologies, challenges remain in addressing automated and intelligent attacks, biases in ML models, and the complexity of high-dimensional data. Paper titled "**Cyber security: performance analysis and challenges for cyber-attack detection.**"

This paper explores the advancements and challenges in cyber security technologies, focusing on using intelligent techniques to detect and respond to cyber-attacks. It addresses the limitations of these approaches and provides an extensive bibliography on the topic. DDoS attacks, identified as a major threat due to their ability to evolve and cause significant damage, are emphasised. The paper also highlights the challenges posed by big data in detecting cyber-attacks, particularly the lack of representative datasets. Using hybrid deep learning models has shown significant progress in enhancing network security and ensuring data integrity. Paper titled "**Ransomware-based Cyber Attacks: A Comprehensive Survey** "Surveys the latest advancements in ransomware detection, focusing on solutions that utilise technologies such as Machine Learning, Deep Learning, Federated Learning, Blockchain, and Software Defined Networks (SDN). It also designs service scenarios for detecting ransomware-based cyber-attacks in IoT applications, focusing on environments like Smart Homes, Smart Industries, and Smart Vehicular Networks. The paper outlines future challenges and directions and proposes developing a novel architecture for ransomware detection in IoT using emerging technologies like Gated Recurrent Units (GRU) and Homomorphic Encryption (HE). Paper titled "**Cascading effects of cyber-attacks on interconnected critical infrastructure.** "This experimental study examines cyber-attack cascading effects on interconnected critical infrastructures, focusing on water treatment and distribution systems. Using an invariant-based approach, distributed invariants were derived to detect anomalies caused by cascading attacks across interdependent systems. The experiments revealed that attackers targeting critical nodes could cause widespread disruption by attacking a pump, such as water service interruptions. The findings highlight the need for distributed invariants, as system-specific invariants alone may fail to detect attacks. Future research will explore the cascading effects between power and water systems and develop integrated safety and security models for interconnected infrastructures.

## 3. Statistics


**Fig. 1. Bar chart illustrating the estimated annual cost of cybercrime worldwide from 2018 to 2028, measured in trillions of U.S. dollars. It shows a sharp rise in cybercrime costs over the years.**

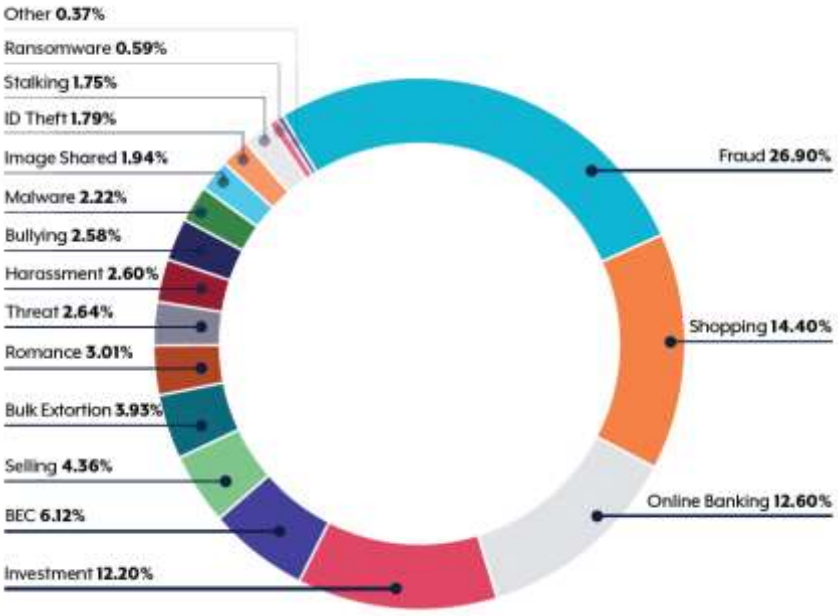


**Fig. 2. Bar chart displays the frequency or percentage of different cyber threats during this period.**

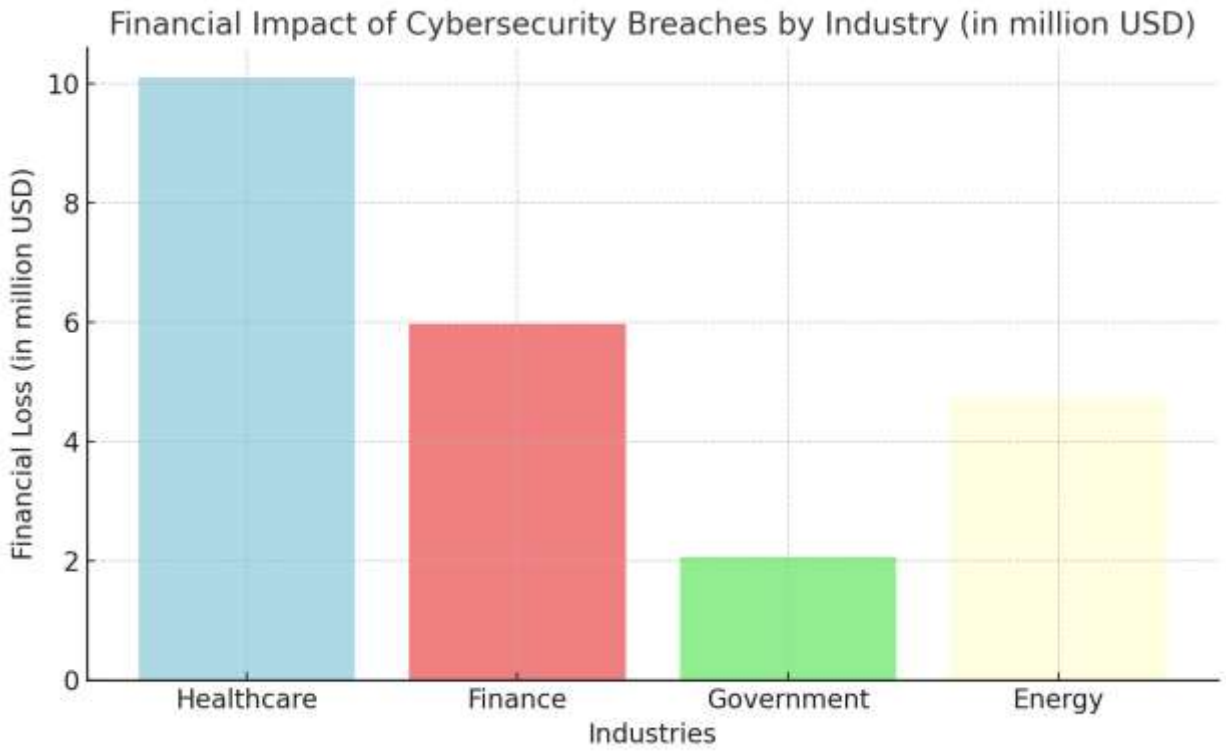


**Fig. 3. Bar chart displays the financial losses incurred due to cybersecurity breaches across four major industries. The y-axis represents financial loss in millions of USD, while the x-axis represents different industries.**

## 4. Timeline of Cyber Attack

**Most common types of Cyber Attacks in 2020**

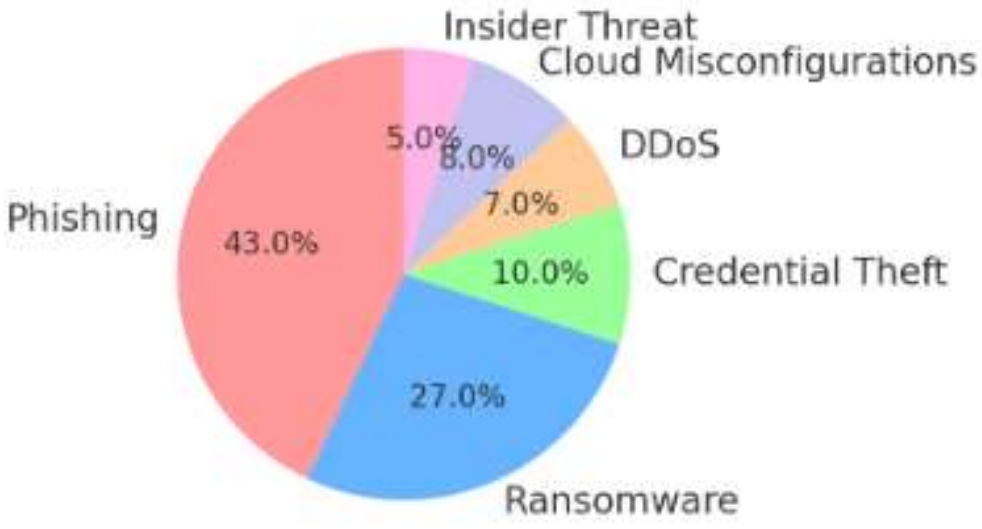


**Fig. 4. Pie chart illustrating the most common types of cyber-attacks in 2020**

In this pie chart of 2020, phishing was the mode of attack responsible for 43% of the breaches, with increased susceptibility as businesses transitioned to remote working environments, mainly using email-based attacks. Ransomware was second, standing at 27%, as the attackers used vulnerabilities in RDP. Credential theft followed third, at 10%, as the attackers pinpointed poor password management. 7% were DDoS attacks, while 8% were cloud misconfigurations where businesses rapidly transitioned to cloud platforms. This incident involved 5 per cent of insiders, and thus, there is a need for even more robust internal security controls against malicious or careless employees.

**2021 Cyber Attacks**

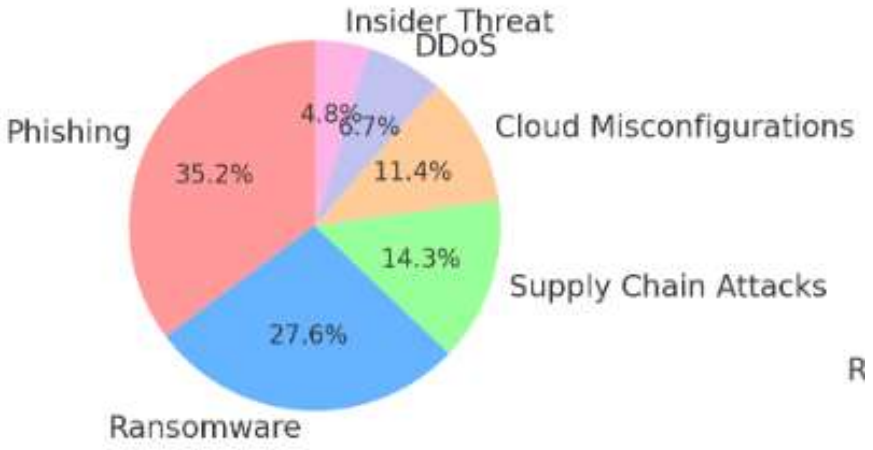


**Fig. 5. Pie chart illustrating the most common types of cyber-attacks in 2021**

In this pie chart, Ransomware shot up to 29% in 2021, with the Colonial Pipeline attack being one of the highest-profile attacks demonstrating its destructive potential. At 37%, phishing was still the top method used for attacks; however, supply chain attacks rose to 15%, significantly impacting smaller businesses. Breaches because of cloud misconfigurations comprised 12% of incidents, given the ongoing migration toward cloud-based infrastructures. DDoS attacks were flat at 7%, whereas insider threats decreased somewhat to 5%, potentially due to increased employee tracking and the implementation of zero-trust policies across organisations.

**2022 Cyber Attacks**

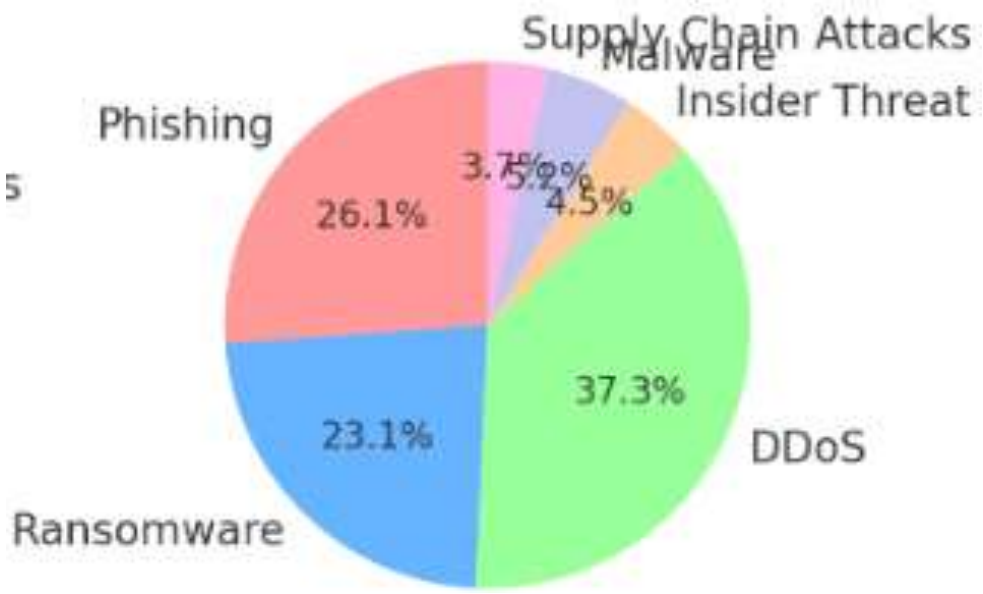


**Fig. 6. Pie chart illustrating the most common types of cyber-attacks in 2022**

In this pie chart, DDoS attacks finally became the most significant headache by 2022, accounting for 50 per cent of incidents because DDoS services are now widely available as a hire service. Ransomware attacks dominated at 31%, while phishing remained a mainstay in 35% of breaches. Insider threats dropped to 6%, showing improved security controls inside an organisation; malware attacks stayed at 7%, and supply chain attacks at 5%. The year has underscored the growing nature of threats through external attack means against business infrastructure.

**2023 Cyber Attacks**

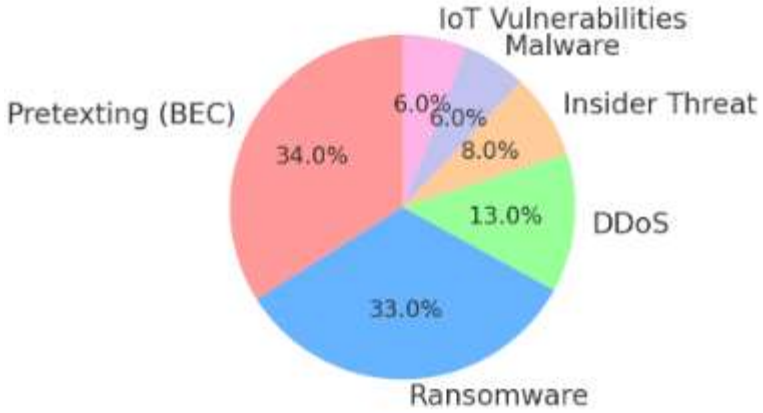


**Fig. 7. Pie chart illustrating the most common types of cyber-attacks in 2023**

In this pie chart, Pretexting had become the leader for Business Email Compromise in 2023, accounting for 34% of breaches, thus displacing phishing. Ransomware stabilised at 33% to ensure it was a non-receding threat. DDoS attacks formed 13 per cent with significant effort towards service disruption. Insider threats still came in at 8 per cent, malware at 6 per cent, but this was when IoT vulnerabilities peaked above 6 per cent as the world embraced IoT with little security preparedness. The year captures well the trend of more complex social engineering attacks and the exploitation of emerging technology.

**2024 Cyber Attacks**

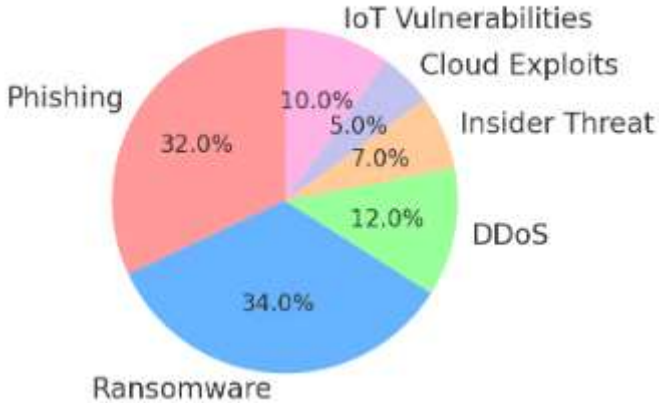


**Fig. 6. Pie chart illustrating the most common types of cyber-attacks in 2024(till September)**

In this pie chart, Ransomware shot up to 34% in 2024, and the growth was even more intense in cloud environments. Phishing decreased by one point to 32%, DDoS attacks to 12%, and IoT vulnerabilities rose for the first time to 10%, with attackers focusing on unsafely secured devices at a high level of network basis. Cloud exploitation occurred at 5% of attacks- a new normal reflecting further penetration of cloud-based services. These 7% of insider threats showcase internal monitoring and the implementation of zero-trust frameworks to fight the adversary from within. Below is the table of significant cybersecurity attacks between 2020 and 2024, when the threat landscape grew across various organisations and geographies. Each represents continuity by cybercriminals and malicious actors in using the existing vulnerabilities for impactful disruption, data breach, financial loss, and operational 9loss, among several ransomware attacks that made headlines in 2020. The Accellion Supply Chain Attack also breached several organisations through supply chains, again showing the burgeoning threat aimed at third-party vendors and suppliers. Of the other alarming trends, the Florida Water Supply Attack had unauthorised access attempted against critical infrastructure to poison the water supply to show vulnerabilities in essential public services. Additionally, Australian Channel 9 News was hacked with ransomware; for this reason, its broadcasting was severely disrupted. The Colonial Pipeline Attack in the United States seriously disrupted fuel supplies nationwide. Since then, it has been among the highest-profile ransomware cases to date. Ransomware attacks, including data breaches, became a significant issue in 2022. This included a highly disruptive ransomware attack against the Government of Costa Rica, a violation at Australian health insurance firm Medibank that had exposed the personal data of millions of customers, and finally, a ransomware attack against the Common Spirit Health System that had seriously disrupted health services in a manner customary for the healthcare industry. On its part, a leak in the gaming sector involving sensitive game data and assets hit Rockstar Games. At the same time, Uber was again breached, leaking sensitive information on customers and drivers. Indeed, the list of sectors on which the attacks fell proved that the attacks in 2022 indeed hit across the board. Throughout 2023, ransomware attacks and data breaches never stopped. Among those was the ransomware-related disruption that hit Johnson Controls and Australian Port Operations. Most prominent among them is that MGM suffered a severe data breach, with the information leakage about its customers. Besides, the retail business has also been hit, with a supply chain attack taking down Dollar Tree, which shows even retail

can't be out of the radar of such attacks. Geopolitical in nature, the Russia-Ukraine Cyberwar showed how cybersecurity attacks by state actors mounted against core infrastructure have further highlighted the role of cyberwar amidst international disputes. The crystal ball for 2024 has sung the same old song: emerging attack vectors rule. The Ivanti VPN attacks have leveraged vulnerabilities in VPN service to compromise several entities operating on remote access solutions. There has been unauthorised access to Microsoft Executive Accounts, with evidence that this has been one of the increasing vectors. Attacks have also used vulnerabilities in Small Office and Home Office routers to strike SOHO Routers. Health was not left behind, too, since Change Healthcare faced a ransomware attack that yet again disrupted health operations. Finally, vulnerabilities in remote access tools were favoured in ConnectWise Screen Connect attacks, creating significant risk for organisations using solutions for remote work.

| **Year** | **Attack Name** | **Attack Vector** | **Impact** | **Source** |
|---|---|---|---|---|
| 2020 | Toll Group | Ransomware | Disruption of logistics and transportation | TechTarget |
| 2020 | Marriott International | Data Breach | 5.2 million guest records compromised | TechTarget |
| 2020 | Magellan | Ransomware | Disruption of healthcare services | TechTarget |
| 2020 | Twitter | Social Engineering Attack | Multiple high-profile accounts hacked | TechTarget |
| 2020 | Garmin | Ransomware | Disruption of GPS services globally | TechTarget |
| 2021 | Microsoft Exchange Attack | Zero-Day Vulnerability | Hundreds of organisations affected globally | BBC ZDNet |
| 2021 | Accellion Supply Chain Attack | Supply Chain Attack | Data breaches across multiple organisations | ZDNet TechCrunch |
| 2021 | Florida Water Supply | Hacking/Unauthorized Access | Attempted poisoning of water supply | The Verge |
| 2021 | Australia Channel 9 News Attack | Ransomware | Broadcasting operations were severely disrupted | Sydney Morning Herald |
| 2021 | Colonial Pipeline Ransomware Attack | Ransomware | Fuel supply disruption in the US | The Guardian |
| 2022 | Government of Costa Rica | Ransomware | Government operations disrupted | Microsoft Digital Défense Report |
| 2022 | Medibank | Data Breach | The personal data of millions of customers is exposed | TechCrunch |
| 2022 | Common Spirit Health System | Ransomware | Disruption of healthcare operations | CNBC |
| 2022 | Uber | Data Breach | Sensitive customer and driver data exposed | TechCrunch |
| 2022 | Rockstar Games | Data Breach/Leak | Sensitive game data and assets leaked online | Polygon |
| 2023 | Johnson Controls Ransomware Attack | Ransomware | Disruption of operations | TechCrunch |
| 2023 | MGM Customer Data Stolen | Data Breach | Personal data of customers compromised | CNN |
| 2023 | Dollar Tree Supply Chain Attack | Supply Chain Attack | Disruption in retail operations | SC Media |

| | | | | |
|---|---|---|---|---|
| 2023 | Australian Port Operations Crippled | Ransomware/Disruption | Port operations halted | The Guardian |
| 2023 | Russia-Ukraine Cyberwar | State-Sponsored Hacking | Disruption in critical infrastructure | BBC |
| 2024 | Ivanti VPN attacks | VPN Vulnerability Exploit | Multiple organisations affected | Bleeping Computer |
| 2024 | Microsoft Executive Accounts Breach | Unauthorised Access | Executive accounts compromised | SecurityWeek |
| 2024 | SOHO Routers Attacks | Router Vulnerabilities | Small office/home office routers compromised | CSO |
| 2024 | Change Healthcare Attacks | Ransomware | Healthcare operations disrupted | Forbes |
| 2024 | ConnectWise Screen Connect Attacks | Remote Access Vulnerabilities | Organisations using remote tools are affected | Bleeping Computer |
| 2024 | Hezbollah Pager Attack | Remotely detonated custom pagers rigged with explosives | 39 killed, 3,400+ injured across Lebanon | Hezbollah organization outfit |
| 2024 | Walkie-Talkie Explosion | Remotely triggered walkie-talkies with embedded bombs | Multiple deaths and injuries in Lebanon | Hezbollah organization outfit |

**Table 1 illustrates one of the most significant cyber-attacks from 2020 to 2024, including their attack vector, impact, and source.**

## 5. Conclusion

The major cybersecurity incident case study from 2020 to 2024 prescribes a dramatically developing landscape of threats that organisations, regardless of the sector they deal with, are about to face. Quite obviously, data breaches compromise millions of personal records, from disrupting logistics and healthcare services to ransomware attacks. It would appear now that the attackers are relentlessly devising innovative ways of causing unprecedented destruction. The increased usage of digital services and interconnected systems widens the attack surface, making critical infrastructure, healthcare, finance, and government sectors so interestingly appealing. One of the trends that has persisted over these years is the predominance of ransomware attacks disrupting services and wreaking havoc on operations. Speaking precisely, the health segment reported on more than one occasion that this hit hard on patient service delivery. Other vital aspects worth noticing are supply chain vulnerabilities in attacks on Accellion and Dollar Tree, where cyber offenders attacked third-party vendors to get to a much more major network. State-sponsored cyberwarfare has also illustrated the geopolitical ramifications of critical infrastructure attacks, as was seen with the Russia-Ukraine cyber conflict. It also describes how attack methods have become increasingly sophisticated: Zero-day vulnerabilities, social engineering, and VPN exploits are rising as adversaries become more technically competent. Increased attacks against SOHO routers and remote access tools show how the shift to working from home opened new doors for exploitation. These emerging threats are making organisations need to implement proactive cybersecurity strategies that include periodic security testing, detailed incident response plans, and extensive employee training on phishing and social engineering. Additionally, embedding supply chain security, active threat detection systems, and critical infrastructure protection are other aspects of any worthy cybersecurity program. Because cyberattacks mount in frequency and sophistication, an approach that works with the world is needed to raise the ante on cyber defence resiliency.

**REFERENCES**

[1] V. R. Palleti, S. Adepu, V. K. Mishra, and A. Mathur, "Cascading effects of cyber-attacks on interconnected critical infrastructure," *Cybersecurity*, vol. 4, no. 1, 2021, doi: 10.1186/s42400-021-00071-z.

[2] A. Bilen and A. B. Özer, "Cyber-attack method and perpetrator prediction using machine learning algorithms," *PeerJ Computer Science*, vol. 7, 2021, doi: 10.7717/PEERJ-CS.475.

[3] K. Kim, F. A. Alfouzan, and H. Kim, "Cyber-attack scoring model based on the offensive cybersecurity framework," *Applied Sciences (Switzerland)*, vol. 11, no. 16, 2021, doi: 10.3390/app11167738.

[4] G. M. Caporale, W. Y. Kang, F. Spagnolo, and N. Spagnolo, "Cyber-attacks, spillovers and contagion in the cryptocurrency markets," *Journal of International Financial Markets, Institutions and Money*, vol. 74, 2021, doi: 10.1016/j.intfin.2021.101298.

[5] H. S. Lallie *et al.*, "Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic," *Computers and Security*, vol. 105, 2021, doi: 10.1016/j.cose.2021.102248.

[6] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, 2021, doi: 10.1016/j.egyr.2021.08.126.

[7] A. H. Matey, P. Danquah, and G. Y. Koi-Akrofi, "Predicting Cyber-Attack using Cyber Situational Awareness: The Case of Independent Power Producers (IPPs)," *International Journal of Advanced Computer Science and Applications*, vol. 13, no. 1, 2022, doi: 10.14569/IJACSA.2022.0130181.

[8] J. Chen, A. J. Gallo, S. Yan, T. Parisini, and S. Y. R. Hui, "Cyber-Attack Detection and Countermeasure for Distributed Electric Springs for Smart Grid Applications," *IEEE Access*, vol. 10, 2022, doi: 10.1109/ACCESS.2022.3145015.

[9] T. D. Le *et al.*, "GridAttackAnalyzer: A Cyber Attack Analysis Framework for Smart Grids," *Sensors*, vol. 22, no. 13, 2022, doi: 10.3390/s22134795.

[10] W. Duo, M. C. Zhou, and A. Abusorrah, "A Survey of Cyber Attacks on Cyber-Physical Systems: Recent Advances and Challenges," *IEEE/CAA Journal of Automatica Sinica*, vol. 9, no. 5. 2022. doi: 10.1109/JAS.2022.105548.

[11] M. Syfert, A. Ordys, J. M. Kościelny, P. Wnuk, J. Możaryn, and K. Kukiełka, "Integrated Approach to Diagnostics of Failures and Cyber-Attacks in Industrial Control Systems," *Energies*, vol. 15, no. 17, 2022, doi: 10.3390/en15176212.

[12] K. S. Jones, N. R. Lodinger, B. P. Widlus, A. S. Namin, E. Maw, and M. Armstrong, "Grouping and Determining Perceived Severity of Cyber-Attack Consequences: Gaining Information Needed to Sonify Cyber-Attacks," *Journal on Multimodal User Interfaces*, vol. 16, no. 4, 2022, doi: 10.1007/s12193-022-00397-z.

[13] J. H. Park, S. K. Singh, M. M. Salim, A. E. L. Azzaoui, and J. H. Park, "Ransomware-based Cyber Attacks: A Comprehensive Survey," *Journal of Internet Technology*, vol. 23, no. 7, 2022, doi: 10.53106/160792642022122307010.

[14] Y. Lyu, Y. Feng, and K. Sakurai, "A Survey on Feature Selection Techniques Based on Filtering Methods for Cyber Attack Detection," *Information (Switzerland)*, vol. 14, no. 3. 2023. doi: 10.3390/info14030191.

[15] O. Gulyas and G. Kiss, "Impact of cyber-Attacks on the financial institutions," in *Procedia Computer Science*, 2023. doi: 10.1016/j.procs.2023.01.267.

[16] Z. Feng, Y. Li, and X. Ma, "Blockchain-oriented approach for detecting cyber-attack transactions," *Financial Innovation*, vol. 9, no. 1, 2023, doi: 10.1186/s40854-023-00490-6.

[17] A. A. Salih and M. B. Abdulrazzaq, "Cyber security: performance analysis and challenges for cyber attacks detection," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 31, no. 3, 2023, doi: 10.11591/ijeecs.v31.i3.pp1763-1775.

[18] I. Fernandez De Arroyabe, C. F. A. Arranz, M. F. Arroyabe, and J. C. Fernandez de Arroyabe, "Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019," *Computers and Security*, vol. 124, 2023, doi: 10.1016/j.cose.2022.102954.

[19] J. Jin, N. Li, S. Liu, and S. M. Khalid Nainar, "Cyber attacks, discretionary loan loss provisions, and banks' earnings management," *Finance Research Letters*, vol. 54, 2023, doi: 10.1016/j.frl.2023.103705.

[20] Ö. Aslan, S. S. Aktuğ, M. Ozkan-Okay, A. A. Yilmaz, and E. Akin, "A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions," *Electronics (Switzerland)*, vol. 12, no. 6. 2023. doi: 10.3390/electronics12061333.

[21] R. Shandler and M. A. Gomez, "The hidden threat of cyber-attacks–undermining public confidence in government," *Journal of Information Technology and Politics*, vol. 20, no. 4, 2023, doi: 10.1080/19331681.2022.2112796.

[22] T. Roy, S. Sattarzadeh, and S. Dey, "Cyber-Attack Detection in Socio-Technical Transportation Systems Exploiting Redundancies Between Physical and Social Data," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 54, no. 3, 2024, doi: 10.1109/TSMC.2023.3328319.

[23] S. H. Oh, J. Kim, J. H. Nah, and J. Park, "Employing Deep Reinforcement Learning to Cyber-Attack Simulation for Enhancing Cybersecurity," *Electronics (Switzerland)*, vol. 13, no. 3, 2024, doi: 10.3390/electronics13030555.

[24] A. Solat, G. B. Gharehpetian, M. S. Naderi, and A. Anvari-Moghaddam, "On the control of microgrids against cyber-attacks: A review of methods and applications," *Applied Energy*, vol. 353, 2024, doi: 10.1016/j.apenergy.2023.122037.

[25] T. Kerdphol, I. Ngamroo, and T. Surinkaew, "Enhanced robust frequency stabilisation of a microgrid against simultaneous cyber-attacks," *Electric Power Systems Research*, vol. 228, 2024, doi: 10.1016/j.epsr.2023.110006.

[26] C. Singh, R. Singh, Shivaputra, M. Tiwari, and B. Hazela, "Analyse and Predict the Detection of the Cyber-Attack Process by Using a Machine-Learning Approach," *EAI Endorsed Transactions on Internet of Things*, vol. 10, 2024, doi: 10.4108/eetiot.5345.

[27] N. Tatipatri and S. L. Arun, "A Comprehensive Review on Cyber-Attacks in Power Systems: Impact Analysis, Detection, and Cyber Security," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3361039.

[28] Verizon, "2024 Data Breach Investigations Report," SOCRadar® Cyber Intelligence Inc., 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/

[29] IBM, "X-Force Threat Intelligence Index 2024," IBM Security, 2024. [Online]. Available: https://www.ibm.com/security/data-breach/threat-intelligence

[30] ENISA, "ENISA Threat Landscape Report 2024," European Union Agency for Cybersecurity, 2024. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threat-landscape