VOLUME - 14, ISSUE - 12, DECEMBER - 2025 • PRINT ISSN No. 2277 - 8160 • DOI : 10.36106/gjra

Original Research Paper

Commerce

CYBER CRIMES AND IMPORTANCE OF ITS PREVENTION IN BUSINESS

Dr. Rajesh S. Sarkate

JES's, R.G. Bagdia Arts, S.B. Lakhotia Commerce and R. Bezonji Science College, Jalna

ABSTRACT

Cyber technologies have largely influenced every part of our lives like education, medical and business. It has provided great comfort in managing data and other resources especially in business areas where customer data, inventory of stock, sales management plays crucial role in deciding future business policies. In contrast, Internet and related cyber threats are emerging as a major concern in recent years. This paper analysis various cybercrimes in business, possible reasons behind and its impact on business. Concern threats for business found are phishing, ransomware, DDoS, data breach etc. Reports have shown that companies, especially small and medium business are not still serious about taking preventive majors against such cyber threats. They are lagging behind in having cyber experts to maintain their digital assets and proper trainings. Also, they need to adopt better policies against data privacy, phishing, and Ransomware attacks.

KEYWORDS :

INTRODUCTION

Currently, Cybercrime has become a major concern that impacts individuals, businesses, and governments. In the era of internet, everyone is significantly relying on use of the internet and digital devices in commerce, government, and daily life. A particular use may be an online payment to a small vendor or huge corporate transactions. Besides, it includes Client relationship management (CRM) to manage and analyse business interactions with its clients to improve communication, satisfaction, inventory management system, a software solution implemented by companies to track orders throughout its lifecycle. Internet has become a lifeline for E-businesses and E-Commerce.

Though, Internet has boosted and eased the business management, it also has brought many threats along with it. Ranging from data threats, company secretes to financial losses, these threats is giving additional bothers to the business industries. This paper has put an insight on various cybercrimes and possible fears to the companies and business organisations.

Cyber Crimes

The 21st century has given new tools for work and data management via cyberspace. While cyberspace is an enabler of progress, it also gives rise to significant cyberspace security challenges. Sometimes, the digital environment is found weaker and invites several attacks called cybercrimes. These cybercrimes are not physical attacks with guns or warfare but attempts to steal, disrupt or gain illegal access to others personal data or critical digital infrastructure with digital devices and tools. It's the offensive process, adopted by a hacker/threat actor, to harm the digital assets of an individual or an organization. The impacting assets could be computers, laptops, networks, servers, information systems, security infrastructures, and many more.

Types of Cybercrimes

- **Malware:** Malware or malicious software are viruses, Trojans, Ransomware, Spyware, etc., designed to gain unauthorized access to computer systems, servers, or networks. Malware can steal, delete, and encrypt data, disrupt business operations, and destroy computer systems.
- **Password Attack:** Password attacks are one of the most prevalent cyber-attacks, in which the attacker employs special techniques and software to hack password-protected files, folders, accounts, and computers.
- **Phishing:** Phishing, the most common form of password attack, is sending fraudulent communications to targets over emails, texts, and calls, while pretending to be from reputable and legitimate institutions. Phishing attacks are generally performed to steal personal user data, login credentials, credit card numbers, etc.

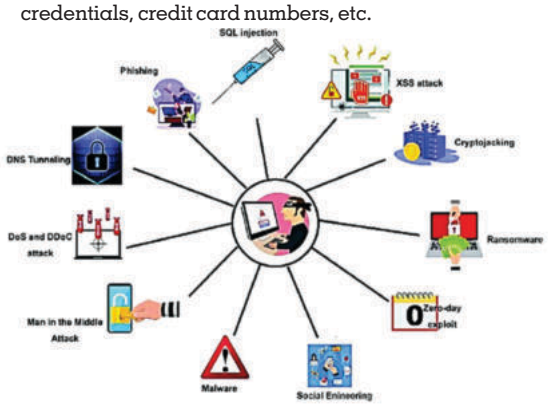

Fig 1 : Types of Cyber Attacks

- **Distributed Denial-Of-Service (DDoS):** DDoS attacks are attempts to disrupt and overwhelm a target website with fake or synthetically generated internet traffic. They are becoming increasingly common and aim to pose serious financial and reputational damages to an organization.
- **Man-In-The-Middle Attack (MITM):** MITM is a kind of eavesdropping cyber-attack where an attacker joins an existing conversation between two legitimate parties, intercepts it, and secretly relays and alters conversations with the malicious intent to steal bank credentials and other financial information of the targets.
- **SQL Injection Attacks** Structured Query Language (SQL) injection is a common method of taking advantage of websites that depend on databases to serve their users. Clients are computers that get information from servers, and an SQL attack uses an SQL query sent from the client to a database on the server. The command is inserted, or "injected", into a data plane in place of something else that normally goes there, such as a password or login. The server that holds the database then runs the command and the system is penetrated.

Motive Behind Cybercrimes in Business

There are numerous motivations behind the execution of cybercrimes, ranging from monetary incentives and corporate espionage to geopolitical ambitions and personal vendettas.

- **Personal Motives:** Certain attacks are driven by personal motivations, often carried out by disgruntled employees or former workers. These individuals may steal sensitive corporate data either to sell it for profit or to sabotage the organization they believe wronged them.
- **Financial Gains:** One of the main drivers of cybercrimes is the potential for financial gain. These attacks are often

inexpensive to execute, despite the possibility of large financial benefits. For instance, the average cost of a data breach has gone to millions.

- **Industrial Surveillance:** Many cybercrimes are motivated by the need for a competitive advantage. Cybercriminals employ phishing as one of their strategies to compromise corporate systems, take over user accounts, and steal critical company data. More complex attacks, such as "whaling," employ well considered strategies to extort companies or steal critical data from key executives.
- **Digital Activism:** Hacktivism is the practice of committing cybercrimes in order to further political agendas. To draw attention to issues like internet censorship, freedom of speech, and government spying, organizations like Anonymous and WikiLeaks have taken aim at governments and big businesses.
- **Adventure Attacks:** Some people commit cybercrimes just for the joy of breaking into systems or for intellectual stimulation. Even though these "white-hat" hackers usually have no malicious intent, their acts can nevertheless seriously impair company operations. Sometimes the goal of ethical hackers is to find security holes and enhance businesses' defences.
- **Easy Targeting of Data:** The simplicity with which hackers can obtain sensitive data is a major contributing factor to cybercrimes. Weaknesses like dormant or expired passwords make it considerably easier for hackers to get access to systems. According to an analysis on data threats, half of corporate accounts are inactive or out-of-date, around 35% of users have passwords that never expire.

Common Myths about Cyber-Security in Business

In business, there are many general myths present about cybercrime in terms of small businesses, antivirus software, and identification of cyber-attack. There are also misunderstanding about sources of cyber threats, use of personal devices and passwords. In reality, cybercriminals target organizations of all sizes, and cyber-security requires a multi-layered approach and continuous effort to manage.

Many small entrepreneurs consider that their very small and cyber attacker will not benefited in any manner. Small businesses are frequently targeted because they often have limited resources and no or fewer dedicated IT security experts. Therefore hackers see them as soft targets. Overall situation makes small businesses more vulnerable for cybercrimes.

Another misconception is that cyber threats are present from outside attackers. But in reality, there is always a possibility that insider are cause of threats. This may be purposely or accidentally but insider can put business on a significant risk. The attacks may enter from disturbed employees or contractors.

The owners especially in small businesses may have an impression that their data is not very important and valuable. In fact, in today's age of information, any kind of data is important. It can be sold, used for identity theft, or to compromise others to scam friends and contacts.

Technical assumptions like "Antivirus-Antimalware software are enough to protect cyber-attacks" will put your organisation on great risk. Though antivirus software are an important aid in security but it alone is not able to protect against sophisticated attacks like phishing attacks, hackers. "Strong passwords will keep my account safe" is another common myth. No doubt, it is important to have a strong, unique passwords. But passwords are only the front layer of protection. Practices of having multi-factor authentication also help in safeguarding your business systems.

Many businesses gives least priority to hire security personals in order to protect their business network systems. As per report, 40% businesses lack security experts. They consider that any normal employees like data entry operators can easily find whether their systems or network are under attack. Modern malware is often stealthy and can remain in dormant phase for long periods, sometimes years,

Few Other Myths in Terms

- As long as there is a password, public Wi-Fi is secure. Truth: Public Wi-Fi networks that are password-protected can still be breached, making it dangerous to access private data on them.
- The IT department alone is in charge of cyber security. Reality: Cyber security is everyone's responsibility. Every user must adopt safe habits and be aware of potential hazards.
- Once company uses security measures, business is secure. In reality, Cyber security is not a one-time endeavour. With new dangers appear, it necessitates ongoing monitoring, updates, and adaption.
- There is no more risk while working from home than when working in an office. In Reality Home networks and personal devices are frequently less secure than corporate networks and can be infiltrated more quickly, especially if they share a network with business devices

Impact of Cyber-Attacks on Business

In Data Theft and Privacy Breaches, Hackers target sensitive information for monetization or to facilitate subsequent attacks, with data theft and privacy breaches posing difficulties beyond immediate losses. As per survey conducted in 2023 by digital Ocean, it is found that 74% of businesses say that data privacy is a top concern for their business, but the majority (57%) have zero employees dedicated to data privacy, with 42% stating they have one to five people focused solely on data privacy.

Furthermore, cyber-security incidents pose severe damages to the reputations, damaging relationships with consumers, partners, and investors and altering stock prices. According to research from the U.K.-based company, companies that experience data breaches suffer from long-term effects on investor confidence and market reputation, as well as an immediate drop in stock price after the breach and ongoing underperformance against the Nasdaq. Around 47% of Consumers has lost the faith and heisted to continue Business With Companies.

Operational overheads comprise several issues that firms often experience, such as system downtime and productivity losses, which can severely impair overall efficiency and output. System disruptions also always result in revenue losses, which adds to the financial burden. Companies can unexpectedly find themselves needing to make emergency hardware or software acquisitions to address these challenges fast. To effectively reduce these operational constraints, comprehensive cyber-security measures and a strong infrastructure are required, as the cost of restoring or rebuilding damaged data and systems adds yet another layer of expenditure.

Immediate overheads linked with cyber-security breaches can be enormous, involving a number of expenses. Cyber-attacks like Ransomware, in 2023, were experience around 21% and are anticipated to cost hundreds of billion yearly by 2031, suggesting a major financial hardship for impacted firms. To effectively manage and mitigate the situation, businesses may also need to invest in cyber-security experts and emergency IT services. Additional considerations include potential fines and legal costs because violations frequently result in complex legal consequences that call for professional help. In order to safeguard and reassure their

customers, impacted businesses may also have to pay for consumer notification and credit monitoring.

The long-term financial implications of cyber-security incidents are enormous, leading to increasing insurance rates and mandating investment in stronger security measures. To reduce possible dangers, companies frequently undertake security awareness and personnel training programs in addition to continuing monitoring and compliance expenses. But still, around 53% of businesses feel that lack of time to focus on security is the biggest challenge

Modern firms depend on interconnected digital supply chains, rendering them exposed to cascading hazards if one link is compromised. Threats to the supply chain are increasing, and breaches frequently start with third-party suppliers. Vulnerabilities in software supply chains can expose thousands of downstream businesses. To lessen these growing risks, companies are spending more on supply chain security and third-party risk management.

CONCLUSION

Given that they frequently affect numerous operational, financial, and reputational aspects, it is clear that cyber-attacks pose a significant threat to businesses and organizations in developed nations. Attacks cause billions of dollars' worth of direct and indirect financial losses each year, while businesses' ability to survive in the digital era is undermined by operational disruption and a decline in customer trust. On the other hand, although many corporations and organizations have begun to offer preventive methods such as relying on sophisticated technologies and building up employee knowledge, businesses often don't have the time or resources, including budget and employees, to dedicate to securing their business. Achieving a balance between technological innovation and security protection is crucial for businesses in developed countries to have a secure and sustainable future.

REFERENCES

1. E. Babulak (2010), The 21st Century Cyberspace, SSRN Electronic Journal, DOI:10.2139/ssrn.3925835
2. Caravelli, J., & Jones, N. (2019). Cyber Security: Threats and Responses for Government and Business. ABC-CLIO.
3. Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security (pp. 63-72). Springer Berlin Heidelberg.
4. Chowdhry, D. G., Verma, R., & Mathur, M. (Eds.). (2020). The Evolution of Business in the Cyber Age: Digital Transformation, Threats, and Security. CRC Press.
5. Corallo, A., Lazoi, M., & Lezzi, M. (2020). Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts. Computers in Industry, 114, 103165.
6. Sakban, A., Kasmawati, A., & Tahir, H. (2020). The role of Indonesian National Cyber Bureau in monitoring mining business companies. In IOP Conference Series: Earth and Environmental Science (Vol. 413, No. 1, p. 012032). IOP Publishing.
7. Tan, Z., Jamdagni, A., He, X., Nanda, P., & Liu, R. P. (2014). A system for denial-of-service attack detection based on multivariate correlation analysis. IEEE transactions on parallel and distributed systems, 25(2), 447-456.
8. Putte, V. D., & Verhelst, M. (2014). Cyber crime: Can a standard risk analysis help in the challenges facing business continuity managers?. Journal of business continuity & emergency planning, 7(2), 126-137.
9. Cybersecurity Statistics and Trends, https://www.varonis.com/blog/cybersecurity-statistics
10. https://www.cloverinfotech.com/10-cybersecurity-myths-that-cyber-criminals-love/
11. The Definitive Cyber Security Statistics Guide [2023 Edition], https://www.thesslstore.com/blog/cyber-security-statistics/, January 25, 2023
12. Small businesses and cyber security, Online survey report by DigitalOcean, https://www.digitalocean.com/reports/cybersecurity-smbs-2023#download