The Impact Of Cyber Security On The Business Organizations

Wasan Alaa Alhamami
Informatics Institute for
Postgraduate Studies, Iraqi
Commission for Computers and
Wasan_alhamami@yahoo.com

Noora Saleem Jumaah
Ministry of Higher Education
and Scientific Research Informatics.
noora.jummah@scrdiraq.gov.iq

***Abstract*—The contemporary digital landscape witnesses a continuous influx of millions of data files, messages, and transactions traversing the Internet and public business networks on a daily basis. The dependable and unequivocal functioning of this expansive electronic infrastructure, upon which our nation relies extensively, is imperative. Indeed, the sustenance of numerous enterprises is heavily contingent upon the assurance of reliable access and secure network environments.**

Within the ambit of our research paper, we undertake a comprehensive elucidation of the concepts encompassing attacks, cybercrime, and cybersecurity. Delving into the historical evolution of these terms, we elucidate the multifaceted challenges inherent in ensuring cybersecurity. Additionally, we provide a meticulous and structured exposition of cybercrime, delineating its various manifestations and implications.

Keywords—Cyber Security, attacks, crime, Business and Security Impacts.

1. Introduction

In recent times, the emergence of novel terms and theories has precipitated a reconfiguration of the conventional understanding pertaining to organizational roles and economic paradigms. Concepts such as e-government, e-business, virtual organizations, network economics, and the Internet of Things (IoT), alongside entities like the Blue Lake Organization, have begun to exert tangible influences on societal dynamics. The Internet and information technology are acknowledged as pivotal components within these frameworks, facilitating their realization. However, this technological advancement has concurrently introduced a spectrum of new challenges and threats, contributing to an environment characterized by pervasive uncertainties across digital domains Evidently, the pervasive integration of technology is manifest in diverse spheres of human activity, including entertainment (e.g., MP3 files, digital cable), transportation (e.g., air navigation, automotive audio systems), pharmaceuticals (e.g., medical records, diagnostic equipment), communications (e.g., cellular telephony, email correspondence), and commerce (e.g., credit card transactions, online retail platforms), among myriad other applications

In contemplating the indispensability of computing devices in daily life and the extent of personal information stored across various systems, including personal computers and external platforms, the imperative for cybersecurity becomes evident. Cybersecurity endeavors to safeguard such information by means of detecting, responding to, and proactively preventing electronic attacks.

Conversely, organizations increasingly find themselves vulnerable to cyber threats, wherein the operations of these entities risk disruption due to malicious cyber activities. Instances of such disruption include Distributed Denial of Service (DDoS) attacks, which incapacitate systems for temporary durations, or instances wherein hackers deploy malicious codes to compromise data integrity or pilfer proprietary information. Such attacks seldom occur in isolation; the repercussions of breaches within one entity have the potential to cascade, disrupting vital services and the supply chain.

A notable aspect of the contemporary digital landscape is the prevalence of nefarious activities, with the Internet comprising a disproportionate volume of spam compared to legitimate content. Opportunistic hackers exploit vulnerabilities within systems, leveraging the widespread adoption of information technology for criminal endeavors, including terrorist activities. The proliferation of information technology and increased international interconnectedness have facilitated the perpetration of such crimes across geographical boundaries, allowing criminals to exploit security vulnerabilities and operate from unconventional locales.

In the manufacturing sector, efforts to mitigate the risks associated with criminal acts and terrorism have been substantial, with extensive investments in computer integration aimed at fortifying facilities against deliberate attacks. However, manufacturing systems remain susceptible to incidental attacks from viruses, worms, and Trojan horses, which have deleterious effects on operational integrity within manufacturing environments.

2. Classification of Cyber.

In the contemporary era, the rapid pace of technological advancement has rendered the optimization of performance through temporal means increasingly challenging. Leveraging the Internet may emerge as the primary recourse in this endeavor. The term "Internet" denotes a vast network of interconnected computers spanning millions of nodes.

While the Internet affords universal access to its services, it also harbors the looming specter of electronic crimes facilitated by its infrastructure. The realm of cyber encompasses a plethora of terminologies, including but not limited to:

2.1 Cybercrime:

Crimes perpetrated through the utilization of the Internet and computer systems to unlawfully acquire goods, identities of individuals, or disseminate malicious software represent instances of cybercrime. Notably, cybercrime transcends the mere utilization of computers as instruments of criminal activity; rather, it encompasses a spectrum of illicit behaviors analogous to traditional criminal acts. Each form of crime, whether cyber or conventional, entails actions or omissions, with ensuing penalties levied by regulatory authorities in response to breaches of established statutes and legal norms. The deleterious impact on personal safety wrought by electronic crimes conducted over the Internet parallels the repercussions of conventional offenses, necessitating heightened awareness and vigilance among legislators, individuals, and law enforcement agencies alike. Given the evolving nature and inherent complexity of cybercrimes, a comprehensive understanding of preventive measures and enforcement strategies becomes imperative to safeguard individuals and communities from potential harm.

Within the cyber realm, crimes perpetrated in the digital domain are perceived as contemporary challenges, characterized by intricacies necessitating nuanced approaches to apprehension and deterrence. It is conceivable to regard cybercrimes through the lens of traditional criminality, wherein the computer serves as the focal point constituting the locus of criminal activity [1]. The delineation of cybercrime encompasses any criminal activity wherein computers serve as a medium, instrument, or objective for the commission of illicit acts. Such crimes are commonly categorized into two distinct classifications:

1- Computer as the primary target: This classification denotes instances where the primary aim is to target computers utilizing other computing systems. Illustrative examples include Denial of Service (DoS) attacks, hacking endeavors, and the propagation of malicious software such as worms and viruses.

2- Computer as a weapon: In this classification, the perpetration of tangible criminal offenses is facilitated through the use of computers. Examples encompass violations of intellectual property rights, instances of cyber terrorism, wire fraud, dissemination of illicit pornography, credit card fraud, and sundry other electronic crimes. These offenses fall within the purview of regulations stipulated by Internet laws aimed at governing electronic activities and safeguarding against their abuses.

2.2 Cyber Security: Cybersecurity constitutes an integral component of contemporary business management practices pertaining to computer systems. Within this framework, the safeguarding of invaluable information stored within these devices against adversarial threats is paramount. Cybersecurity mechanisms are engineered to thwart attempts aimed at compromising, vandalizing, or illicitly accessing such information, thereby ensuring its integrity and confidentiality. By proactively detecting and responding to a myriad of online attacks, cybersecurity protocols serve to fortify the protection of sensitive business and personal data, including public information.

In light of the imperatives of cybersecurity, internet users are advised to exercise vigilance prior to divulging any personal data, such as name, email, or other personal details, on websites. The presence of a website's privacy policy should be ascertained as a preliminary step in this regard. Furthermore, encryption methodologies play a pivotal role in shielding users from potential data theft, necessitating the adoption of encryption protocols for sensitive information transmission. Secure Sockets Layer (SSL) encryption is commonly employed across numerous websites to fortify the protection of transmitted data.

Moreover, the implementation of updated software and robust password practices is advocated to bolster privacy protection measures. The adoption of complex, difficult-to-guess passwords enhances the resilience of data against incursions by malicious actors. Additionally, refraining from enabling password-saving functionalities on computers and intermittently disconnecting from the internet during periods of device inactivity are recommended practices to mitigate security risks.

2.3 Cyber Attacks: In the contemporary landscape, an extensive volume of information traverses the Internet, rendering it susceptible to an array of cyber threats. Notably, certain cyber-attacks exhibit nuanced behaviors that pose challenges in early detection, thereby complicating mitigation efforts during the nascent stages of these attacks. Motives behind cyberattacks may vary, ranging from deliberate intent to clandestine actions executed without explicit knowledge. Cybercrime manifests through intentional attacks, engendering significant societal repercussions across multifarious domains including psychological distress, threats to national defense, and economic destabilization. Mitigating the proliferation of such electronic crimes' hinges upon a comprehensive analysis of their behavioral patterns and an understanding of their multifaceted impacts across diverse strata of society.

3. History of Cyber Crime

Since the onset of the digital age, criminals have increasingly turned to computers as instrumental tools in perpetrating their illicit activities. Leveraging the capabilities of computers, these individuals employ sophisticated techniques to engage in counterfeiting and circumventing security measures. The advent of computer technology has afforded criminals a level of anonymity previously unattainable in conventional society. With the proliferation of the Internet, offenders capitalize on this anonymity to orchestrate crimes from remote locations. Exploiting the interconnectedness facilitated by the Internet, criminals can breach systems situated continents away, pilfering personal information, credit card details, and banking credentials without the need for physical presence at the targeted location.

The utilization of computers extends to a plethora of criminal endeavors, including but not limited to child trafficking, dissemination of illicit pornography, drug trafficking, and perpetration of bank fraud. Moreover, criminals converge into electronic syndicates spanning across geographical boundaries, leveraging the expertise of individuals proficient in database infiltration and theft. Typically, these offenders adopt "NIC's" or "handles" to conceal their identities while operating within the digital realm

4. Cyber Crime Methodology

Cybercriminals employ various methodologies honed through experience to execute their illicit activities within the digital domain. Leveraging their expertise, these individuals adeptly breach computer systems, utilizing complex computer networks that pose challenges to identification by legal authorities. The clandestine nature of these networks renders the task of pinpointing the perpetrators of cybercrime arduous.

A common tactic utilized by cybercriminals involves hacking into the computers of targeted individuals or victims. To obfuscate their tracks and mask their identities, perpetrators often conduct these nefarious activities from internet cafes or public places, thereby further complicating the process of detection and attribution by law enforcement agencies.

The outlined methodology delineates the sequence of actions typically undertaken by cybercriminals during illegal activities involving computer systems. It unfolds as follows:

a. Intelligence Gathering: Hackers initiate the process by collecting intelligence information pertinent to their illicit objectives.

b. Network Scope Assessment: This phase involves acquiring an understanding of the breadth of networks and their external connections.

c. System Vulnerability Identification: Hackers proceed to identify weaknesses within systems through host enumeration activities.

d. Network Discovery: A comprehensive assessment of the network is conducted to ascertain the types and number of operating systems employed within the targeted victim's computer network.

e. Exploitation of Weaknesses: Exploiting the identified vulnerabilities, cybercriminals gain unauthorized access to the network.

f. Password Cracking: Cybercriminals deploy password cracking programs within the network environment to circumvent user authentication mechanisms.

g. Installation of Spyware: Upon successful penetration of the network, criminals install spyware to surreptitiously capture sensitive information such as passwords and users Identifications.

h. Information Concealment: In certain instances, hackers resort to information hiding techniques to obfuscate their activities and mislead law enforcement agencies.

i. Utilization of Automated Programs: Cybercriminals leverage automated programs to streamline the process of concealing information, facilitating evasion of detection and mitigation efforts.

This systematic approach underscores the sophistication and strategic acumen employed by cybercriminals in orchestrating illegal activities within digital environments

5. Types of Cybercrime

Cybercrimes encompass a diverse array of illicit activities within the digital realm, which can be classified into the following categories:

a. **Hacking/Cracking:** Involves unauthorized access to computer systems or networks, often with the intent to breach security protocols or manipulate data.

b. **Exploitation of Children in Pornography:** Perpetrators utilize the accessibility of the internet to exploit and sexually abuse children, disseminating pornographic content across various online platforms.

c. **Denial of Service (DoS)** Attacks: Entails flooding the victim's network or domain with a deluge of illegitimate traffic, thereby rendering services inaccessible or disrupting normal operations.

d. **Computer Sabotage/Cyber Sabotage:** Refers to the deliberate destruction or alteration of data within computer systems, distinct from theft or misuse.

e. **Propagation of Viruses**: Involves disseminating malicious software, including Trojan horses, web theft, mail bombing, worms, and viruses, which can compromise the integrity and functionality of targeted systems.

f. **Software Piracy**: Encompasses the unauthorized copying, distribution, or counterfeiting of proprietary software products, infringing upon intellectual property rights.

g. **Cyber Terrorism**: Involves utilizing digital platforms to orchestrate terrorist activities, such as distributed denial of service (DDoS) attacks, dissemination of hate mail, or compromising sensitive computer networks to facilitate terrorist agendas.

h. **Trafficking: Encompasses** the illicit trade of weapons, humans, drugs, and other commodities facilitated through online channels, exploiting the anonymity and reach afforded by the internet.

i. **Cheating and Fraud**: Encompasses deceptive practices aimed at defrauding individuals or entities online, spanning fraudulent schemes, identity theft, phishing scams, and other forms of online deception aimed at financial gain.

6. The Security Problems.

One of the biggest concerns is what if there is a hack into the critical systems in government, companies, financial institutions etc. This could lead to malware in critical systems leading to data loss, misuse or even killing the critical systems. In the world of Cyber security, it is expected that some of the following things will be happened:

a. Threats will continue to become more intense. Global competition for business will include efforts to develop and acquire intellectual property. Therefore, intellectual property and intellectual capital will become more valuable than ever before and the threat to them will rise.

b. Also, threats will continue to become more adaptive and subtle. Instead of knowing that a threat has a signature or fingerprint, it will have a changing signature and set of fingerprints, becoming more difficult to detect.

c. Attention to cyber security will rise. Savvier companies realize they need to protect their intellectual property. It won't be a question of compliance – it will be a question of survival.

d. Nations will increasingly cooperate to improve the global economy's cyber security. They will do this to make it more predictable and less susceptible to cyber terrorism and cyber vandalism, as well as protect the critical infrastructures of sovereign countries.

e. More and more of the international cooperation will take place.

f. Policies will emerge that relate to global cyber governance.

7. The Proposed Solutions.

The prevalence of privately owned information companies underscores their emphasis on prioritizing customer satisfaction and fostering positive user experiences, rather than singularly focusing on addressing transnational crime concerns. Noteworthy on the horizon are several emerging cyber developments:

a. Morphological awareness .represents a significant advancement aimed at aiding companies in comprehending the global landscape and internal dynamics of their organizations. This capability enables proactive identification of emerging threats and their evolving patterns, empowering companies to preemptively address potential risks before they impact their operations. This proactive approach, facilitated by situational awareness, fosters resilience and adaptability in navigating complex and dynamic business environments.

b. Developing advanced computer-assisted tools that allow companies to analyze the threat effectively and quickly to choose the appropriate defense best suited to it.

c. The advent of advanced security developments has facilitated the protection of novel infrastructures, including cloud-based systems. Many institutions are increasingly adopting cloud architectures due to their considerable advantages. However, security remains a paramount concern. Nonetheless, the emergence of Trusted Cloud and enhanced cloud security capabilities empowers these institutions to devise and implement new secure architectures. This proactive approach ensures the integrity and confidentiality of data within cloud environments, thereby fostering trust and confidence in the adoption of cloud technologies.

d. In the forthcoming era, social engineering attacks are poised to emerge as the predominant trend in cyber threats. Attackers will increasingly employ sophisticated social engineering tactics to circumvent technological security measures and controls. Leveraging psychological manipulation, these attackers will exploit inherent human tendencies to deceive individuals and gain unauthorized access to sensitive information or systems. This trend underscores the critical importance of cybersecurity awareness and education to mitigate the risks posed by social engineering attacks.

e. Social media has become an enticing platform for cybercrime, particularly as numerous companies incorporate it as a fundamental component of their marketing strategies. However, this adoption presents challenges for businesses in striking a balance between compliance-based obligations, potential litigation risks, and the imperative to actively engage in communication within social communities. Achieving this balance entails navigating the complexities of regulatory requirements while effectively managing the inherent risks associated with social media activities, all while ensuring ongoing participation and interaction with online communities.

f. The human element remains the Achilles' heel in cybersecurity. Criminal actors persist in their belief that they can exploit employees' vulnerabilities, irrespective of technological advancements. The period spanning 2014-2015 witnessed a notable escalation in the sophistication of such human-centric attacks, a trend expected to persist and potentially intensify in the future.

g. Memory Scrapping. Will become more common in the coming time. This has been around for a long time but is more aggressively targeting data such as credit card records, passwords, PIN's, keys, as of late.

h. Wireless adoption will continue, branching out into a larger number of purpose-focused protocols that fit the needs of individual technology. Based on the failed protocols exposure, and the trend of Wi-Fi failure and improvement, we will see history repeating itself where vendors are quick to the market to capitalize on new opportunities, failing to critically examine the lessons from earlier wireless technologies.

i. More cloud Computing Issues will be at the eye of the cyber attackers. Many organizations will soon discover that they do not have the flexibility they need for their business, and many others will discover that any security issues (from audit to compromise) are far more complex in the cloud. Security professionals will continue to apply extra security to scenarios that involve processing sensitive or regulated data in shared cloud environments.

j. Security Continues to become part of Virtual Infrastructure. As more and more organizations add virtualization technologies into their environment, particularly server and desktop virtualization, security will be more embedded in the native technologies, and less of an "add-on" after the implementation is complete. For server virtualization, new firewalls and monitoring capabilities are being integrated into some of the leading platforms now.

8. Conclusion

In this research paper, the focus extends beyond a mere elucidation of cybercrimes; rather, it encompasses an exploration of their ramifications on diverse business entities. Through an exhaustive analysis, this paper elucidates the significance of safeguarding critical information online, which is increasingly susceptible to electronic attacks. By delving into the behavioral patterns of cybercriminals and comprehending their modus operandi, insights are garnered into the multifaceted impacts of these crimes on society at large.

The elucidation of these impacts serves as a cornerstone for devising effective strategies aimed at mitigating and addressing cybercrimes. By comprehensively understanding the behavioral dynamics of cybercriminals and discerning the far-reaching consequences of their actions, stakeholders are equipped with the requisite knowledge to implement proactive measures aimed at fortifying cybersecurity defenses and safeguarding invaluable digital assets.

References

[1] Stephen Northecutt et al (2011), Security Predictions 2012 & 2013- The emerging Security Threat, available at: http://www.sans.edu/research/security-laboratory/article/security-predict 2011, visited 15/10/2012.

[2] Kevin G. Coleman (2011), Cyber Intelligence: The Huge Economic Impact of Cyber Crime, available at: http://gov.aol.com/2011/09/19/cyber-intelligence-the-huge-economic-impact-of-cyber-crime/, visited 5/10/2012.

[3] Bowen, Mace (2009), Computer crime, Available at: http://www.guru.net/, visited 12/10/2012.

[4] DSL reports (2011), Network Sabotage, Available at: http://www.dslreports.com/forum/r26182468-network-sabotage-or-incompetent-managers-trying-to-, visited: 5/10/2012.

[5] Shantosh Rout (2008), network Interference, Available at: http://www.santoshraut.com/forensic/cybercrime.htm, visited 8/10/2012.

[6] Crime Desk (2009), Million Online Crimes in the year: Cyber Crime squad Established. Available at: http://www.the londondailynews.com/million-online-crimes-year-cyber-crime-squad-established-p-3117.html, Visited 12/10/2012.

[7] Power, R, 2001, 2001 CSI/FBI Computer crime and Security Survey, Computer Security Issues and trends, 7(1): 1-18.

[8] Al-Hamami Alaa Hussein and Al-Sadoon Gossoon M. (2014), Editor of “Threat Detection and Countermeasures in Network Security”, Published in the United State of America, Hershey, PA: Information Science Reference (an imprint of IGI Global), ISBN; 978-1-4666-0191-8, 2012, October 2014, Web-site: http://www.igi-global.com.