DE JURE NEXUS LAW JOURNAL

Author:

Sonakshi Kathuriya

Graphic Era University, Dehradun

1st Year, B.com (Hons.)

IMPACT OF CYBERSECURITY ON BUSINESS ENVIRONMENT

Abstract:

Cyber security is a hot topic right now, with a focus on defining the cyberspace or cyber danger. The main focus of this article is to make the readers acquainted about the dilemma faced by cybersecurity and to make them known of the possible attacks and cyber threats that are hitherto present in the Information Technology horizon or cyberspace. The societal landscape is exposed to an abundant number of digital risks and threats on a regular basis. So, it becomes essential not just to identify such quandary and threats but most importantly formation and application of the effective regulations concerning the mitigation of such probable problems. Significant progress has been made in research and development but adding to that the pros that are being brought up by this process, we've to be aware of its demerits too. An undeclared war sis being fought by the global south and the most developed countries as currently it can be seen that they are trying to outcompete each other in global south.

Keywords: *Cyber security, cyberspace or cyber danger, cyber threats, Information Technology, in research and development, global south, global south.*

Introduction To Cybersecurity And Cybernetics

In the words of Russel Schrader, "*cybersecurity is an economic and security issue that can be best addressed through cooperation between private as well as public partnerships with the consumers,*

industry and the government." [1] Small business enterprises as compared to large scale businesses are, however relatively, more vulnerable to cybersecurity attacks since they do not take substantial steps to defend themselves. Small firms may not have the technological tools, financial resources, or legal understanding to defend themselves. Training must be provided via educational seminars so that individuals are aware of how to deal with cyber-attacks.

Cybernetics is a science that deals with quantitative organized concerns of administration, monitoring, and control of self-regulating systems, or a scientific subject that deals with them.[2] One of the branches of cybernetics is cyber security, often known as information technology security. It is utilized in the context of computers and numerous networks that civilization uses on a regular basis. Its main purpose is to safeguard information owners from illegitimate or unlawful behavior.[3]

What has caused the importance of cyber security to rise in recent years?

The rationale is straightforward. Previously, all vital information was kept on paper. The process of electronification, on the other hand, gradually renders the data more sensitive to attacks. Cyber security is a topic that is explored in depth, particularly in industrialized nations. Both the United States of America and Europe are advanced nations that have positioned themselves as security leaders.[4] Despite their unfavorable political, social, and economic circumstances, certain nations, like as Brazil, might be deemed unique in their aggressive efforts to achieve cybernetic safety. Large unrest in 2013 and massive hacking attacks between 2008 and 2012 heightened interest in resolving Brazil's safety issues. Antivirus systems (computer programs) are now the most well-known and are designed to detect and eliminate potential hazards in the digital realm. There are an

[1] Innefu.com. n.d. *HOW CYBER SECURITY IMPACTS BUSINESSES GLOBALLY?*. [online] Available at: <https://www.innefu.com/blog/how-cyber-security-impacts-businesses-globally/> [Accessed 17 March 2022].
[2] Cybersecurity.cz. 2017. *CyberSecurity.CZ*. [online] Available at: <https://www.cybersecurity.cz/basic.html> [Accessed 17 March 2022].
[3] Koraus, A., 2018. *CYBER SECURITY AS PART OF THE BUSINESS ENVIRONMENT*. [online] Research Gate. Available at: <https://www.researchgate.net/profile/Anton-Koraus-2/publication/326211242_CYBER_SECURITY_AS_PART_OF_THE_BUSINESS_ENVIRONMENT/links/5b3e650daca272078514b5af/CYBER-SECURITY-AS-PART-OF-THE-BUSINESS-ENVIRONMENT> [Accessed 17 March 2022].
[4] Koraus, A., 2018. *CYBER SECURITY AS PART OF THE BUSINESS ENVIRONMENT*. [online] Research Gate. Available at: <https://www.researchgate.net/profile/Anton-Koraus-2/publication/326211242_CYBER_SECURITY_AS_PART_OF_THE_BUSINESS_ENVIRONMENT/links/5b3e650daca272078514b5af/CYBER-SECURITY-AS-PART-OF-THE-BUSINESS-ENVIRONMENT> [Accessed 17 March 2022].

abundant number of antiviruses such as Norton, AVG, Avast and McFee, etc. are available in the market to avoid or lessen down the threats to the security of the computers.

Individual systems defend the digital age; nonetheless, it is critical to emphasize that the present state of cyber security is mostly led by users, who often use easy passwords and so subject their systems to increased risk. Consequently, becoming a target of hackers and get their data leaked and abused.

Risk Management In Cybersecurity

Management of risk is critically important component in cybersecurity. The activities and operations of your organization, as well as your consumers, may be jeopardized if your systems, connections, and devices are susceptible.[5] After hearing about the term cyber risk again and again, one must come across the question as what is cyber risk? Therefore, any risk of monetary loss, interruption, or harm to your organization that might be caused by your web behavior, online trade, failure of your IT systems and networks (regardless of cause), or the storing of private information on IT network systems is referred to as ***cyber risk***.[6] Any organization can be affected by the cyber risk which are reliant upon the web systems, information and digital technology.

Assessment of Cyber Risk

The detection, analysis, and evaluation of cyber-threats are involved in the cyber risk assessment. You should view at your total IT foundation as a feature of the assessment and endeavor to reveal potential dangers coming about because of weaknesses in your frameworks, as well as individuals, cycles, and innovation. Also, one should not ignore the all the kinds of cyber threats posed by numerous types of cyber security attacks. While dissecting digital dangers, it's normal to focus on the most basic dangers in view of the opportunity of their event and the expense/effect of their event.

"Exercise in a Box" is a freeware online tool offered by the National Cyber Security Centre in UK to assist the businesses analyze their cyber resilience and practice their reaction in a secure

[5] Nibusinessinfo.co.uk. n.d. *Cyber security risk management | nibusinessinfo.co.uk*. [online] Available at: <https://www.nibusinessinfo.co.uk/content/cyber-security-risk-management> [Accessed 17 March 2022].
[6] Nibusinessinfo.co.uk. n.d. *Cyber security risk management | nibusinessinfo.co.uk*. [online] Available at: <https://www.nibusinessinfo.co.uk/content/cyber-security-risk-management> [Accessed 17 March 2022].

environment. There are many articles available on the web to understand the cyber risk assessment methodology.

What is cyber risk management?

The process which includes the identification, analyzation, evaluation and addressing of the potential organization's cyber security threats is referred to as the cyber risk management. Anything that comes before the risk management of cyber threats is cyber risk assessment. This will provide you an overview of the dangers that might jeopardize your company's cyber security, as well as their severity.

The cyber risk management plan establishes how to prioritize and react to such hazards depending on the organization's appetite for risk.[7]

Process of Cyber Risk Management

A risk management plan often follows these phases, however particular approaches vary.

- Determine the threats to your cyber security. This for the most part involves identifying your framework's network safety defects as well as the dangers that might take advantage of them.
- Every risk's severity is analyzed by assessment of it's likely occurrence and how serious the consequences will be if it occurs.
- Evaluation of each risk in accordance with the risk appetite of the organization.
- Prioritization of the risks.
- Decision as to the response to risks either they shall be treated, tolerate, terminated or transferred.

Source: Internet Material, www.itgovernance.co.uk

[7] Itgovernance.co.uk. n.d. *Cyber Risk Management | IT Governance UK*. [online] Available at: <https://www.itgovernance.co.uk/cyber-security-risk-management#:~:text=What%20is%20cyber%20risk%20management,is%20a%20cyber%20risk%20assessment.> [Accessed 18 March 2022].

- Since it's a continuum process, the organizations must make sure the monitoring of the risks as if they're still acceptable, controls should be reviewed to make sure that they still fit for the purpose and the changes should be taken place.

Cyber Threats to Business Organizations

We are all members of a knowledge-based society, this has a favourable influence on economic growth on both a national and global scale. On either side, one of the disadvantages of the process of establishing a knowledge society is that we are becoming increasingly reliant on numerous systems, making us vulnerable to cyber-attacks with the potential to do significant damage. According to Green, *"a cyber-attack as an electronic attack on systems of several various companies or organizations, resulting particularly in stealing their accessible assets stored in form of accessible digital information."* [8] (Green, 2016)

Industries in the domains of power, transport, finance, infrastructure, banking, medical services, sewerage and potable water delivery systems, or digital infrastructure are the most typical targets of cyber-attacks nowadays (e-shops, clouds, etc.).

The evolution of cyber dangers is expected to accelerate at a breakneck pace. It is projected that future cyber assaults would primarily target backup storage systems of major corporate enterprises, maybe with the competitive goal of undermining their objectives and causing damage. Users' proclivity for clicking on dangerous URLs in their e-mail boxes is one of the most recent concerns. The credentials may be decrypted, and a system assault can be facilitated with only one click. The image below depicts the geographic distribution of cyber threats in 2016-2017.

Figure 2: Threats from Cybernetics in The World

[8] Green, J., 2016. *Cyber warfare*. 1st ed. Routledge, p.196.

Source: Internal material CISCO, 2017

Top Internet Threats That Include:

- Leakage of information and illicit or unauthorised access to the systems,
- Data tampering: deletion, tampering, or manipulation of data,
- DOS (Denial of Service attacks) and denied access to the systems (ransomware and Trojans)
- Use of information for the illegitimate purpose by an illegitimate person.

Possible Impacts of Cyber Threats on Business

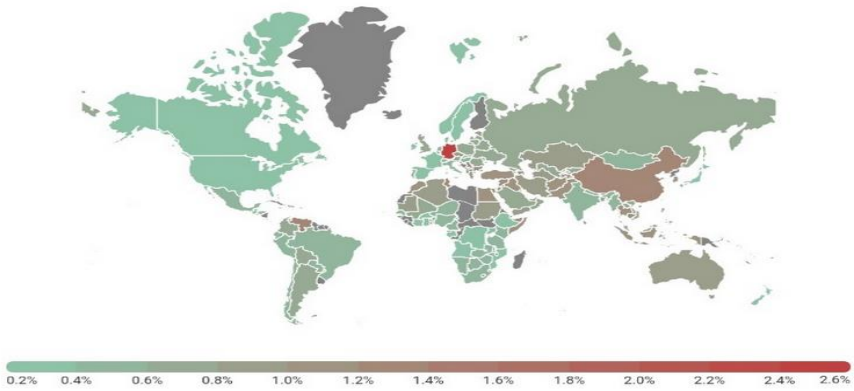
Increased Costs: Organizations who wish to protect themselves against web crooks should dive deep into their pockets. Customarily, to be consistence with online protection necessities, firms might have to draw in legal counselors and different legal experts. Moreover, assuming they are the objective of an attack, they might be compelled to pay much more in lawful expenses and harms as an outcome of common procedures brought against the organization.

Disruption of Operations: Organizations regularly bring about pointless costs from assaults, for example, the probability of a significant stoppage in tasks, which might bring about lost pay, notwithstanding direct monetary misfortunes. Cybercriminals may stifle a company's usual operations in a variety of ways. Assumed "hacktivists," who have been known to enter the PC of associations of government substances or overall relationship for raising an evident shamefulness or propelling straightforwardness, as to disturb business as usual.

Damage of Reputation: Organizations whose brand value is hurt because of significant hacks might experience extreme harm. Consumers and even providers may be wary of entrusting their sensitive data to a firm whose IT system has been breached at least one time. Following an assault, the stock prices of compromised firms decreased an average of 3.5 percent, underperforming the Nasdaq by 3.5 percent.[9]

There are many more consequences that a business organization may undergo after a cyber attack performed on its operations and networking systems. Hacktivism handcuffs the normal operations of the multinational organisations.

Figure 3: Parts of the planet inflicted by malware.



Source: Kunc, 2017[10]

Indian Legislation On Cybercrimes, Every Organization Should Know

Because of the increasing rise of e-banking and e-commerce, financial and personal details must be disseminated in the virtual environment on a regular basis. One of the most significant drivers to India's economic prosperity has been the virtual IT industry. The Indian government created the ***National Cyber Security Policy*** in 2013 with this in mind.

[9] Comparitech. n.d. *How data breaches affect stock market share prices - Comparitech*. [online] Available at: <https://www.comparitech.com/blog/information-security/data-breach-share-price-analysis/> [Accessed 18 March 2022].

[10] Aktuálně.cz - Víte, co se právě děje. 2017. *Grafika: Jak se kradou informace. S kybernetickým útokem má zkušenost 80 procent evropských firem | Aktuálně.cz*. [online] Available at: <https://zpravy.aktualne.cz/zahranici/evropsky-parlament/ohrozeni-kyberneticke-bezpecnosti-v-eu/r~71046d28c47e11e79121ac1f6b220ee8/?redirected=1512766051> [Accessed 18 March 2022].

This policy is continuously being developed, with the goal of becoming a complete platform that covers people, organizations, and quasi organizations. In addition, the strategy **aims** to improve cyber awareness, eliminate supply chain connections, and establish a National Nodal Agency to secure and organize critical information across all enterprises and people. It also aims to provide various types of **businesses the ability to tailor their cybersecurity policy to fit their needs.** It necessitates those businesses set aside a specified budget in order to implement a security strategy in the event of an emergency. As a result, understanding current cyber regulations is critical for every contemporary business organization. It is crucial so as to ensure the smooth functioning of the business operations.[11]

Conclusion and Suggestions

We live in a digital world that is always evolving, introducing new trends, successes, tools, technologies, and so on. The globe is progressively becoming comparable to a civilization that cannot exist without technology. People utilize a variety of social media sites on a regular basis to convey their sentiments, feelings, moods, and sensitive or confidential information. In this world of internet, we quite often become the victim and get abused by those who are using it for their own benefits and purposes. We are all connected to the internet and are so impacted by numerous networks and mediums.

This is the advent of digitalization. Every organization and individual must strive to bring upon the best security practices to save their confidential information and data from a cyber threat or a breach. They must be aware of the terms such as phishing, DOS, SQL injection and trojan, etc. along with the governmental policies on activities such as cyber vandalism, cyber terrorism, cyber pornography and intellectual property crimes. All the business organization must form their own internal cyber security policy with adherence to the legislations by having a legal team in the organization to ensure a smooth professional working climate.

[11] SecureNow. 2021. *India's cyber laws every organisation should be aware of - SecureNow*. [online] Available at: <https://securenow.in/insuropedia/cyber-laws-in-india-every-organisation-should-be-aware-of/> [Accessed 18 March 2022].