The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2024
Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

ENTERPRISES AT THE CROSSROADS: THE CONTINUALLY CHANGING CYBERSECURITY THREAT LANDSCAPE

Can the area of cybersecurity ameliorate at a rate that keeps up with the ever- changing world of digital threats?

The realm of cyber threats has expanded significantly in recent times. The sphere of lone hackers looking for attention, organized crime syndicates, state- sponsored entities, and cybercriminals now make up this complex ecosystem. Their goals gauge from fiscal benefit to spying and the destruction of vital structure. It’s especially concerning that ransomware attacks are on the rise. Malicious associations occasionally cipher victims' data and demand preservations to unlock it. Among the high- profile targets are hospitals, metropolises, and significant associations; this causes significant fiscal losses as well as detriment to a brand. Although the development of technology has made our lives better, it has also made cyber more vulnerable to threats. Cybercriminals now have a larger attack face thanks to the adding use of mobile devices, cloud computing, and the Internet of Things. For hostile individualities, every connected device becomes an implicit point of entry[1].

The threat landscape evolves daily as new cyber threats appear. The following are the primary causes of the dynamic threat landscape

- increasingly advanced instruments and techniques of attack;
- increased dependence on IT goods and services, including SaaS offerings;
- networks, like the dark web, that support and facilitate the distribution of proceeds from cybercrime;

[1] Pedro Ferreira, Cybersecurity at the Crossroads - Can It Keep Up with Threats, Finance Magnates (Jan. 17, 2024), https://www.financemagnates.com/fintech/cybersecurity-at-the-crossroads-can-it-keep-up-with-threats/

- increased financial, human, and skill availability to support cyberattacks;
- outside variables, like a worldwide epidemic or a financial crisis;
- hastily software updates with further features;
- innovative hardware advancements, like Internet of Things widgets

A well- thought- out Incident Response Plan is a necessary element of cybersecurity procedures and proper planning, as it helps IT teams react appropriately in the event of a security breach. “What threats must their company be on alert over?" is a common question posed by IT teams and business directors.

Ten significant cybersecurity threats

1. Ransomware & Malware
2. Endpoint Attacks
3. Phishing
4. Third- Party and Supply Chain Attacks
5. Machine Learning and Artificial Intelligence Attacks
6. IoT (Internet of Things) Attacks
7. Inadequate Patch Management
8. Form jacking
9. Cryptojacking
10. A Severe Shortage of Cyber Security Professionals

Legal Aspects

The main piece of legislation pertaining to cybersecurity, data protection, and cybercrime is the Information Technology Act of 2000. Its salient characteristics are

- Furnishing electronic transactions and communications with legal recognition and protection
- Attempting to protect electronic data, information, and records
- Precluding unauthorized or illegal use of computer systems

- Designating as crimes hacking, denial- of- service attacks, phishing, malware attacks, identity theft, and electronic theft.

The IT Act's rules and regulations govern the following various angles of cybersecurity

- The Computer Emergency Response Team (CERT- In) was created as the administrative body in charge of gathering, analyzing, and sharing data on cybersecurity incidents as well as implementing emergency response measures by the Information Technology Rules, 2013. In addition, intermediaries and service providers are required by these regulations to notify the CERT- In of cybersecurity incidents.
- The 2022 CERT- In directions on information security procedures, practices, prevention, response, and reporting of cyber incidents for a secure and reliable internet supplement and amend the 2013 regulations' existing cybersecurity incident reporting requirements.
- Companies that process, collect, store, or transfer sensitive personal data or information are required to put reasonable security practices and procedures in place under the Information Technology Rules, 2011.
- In order to preserve safe harbor protections, intermediaries must implement reasonable security practices and procedures to secure their computer resources and information, according to the Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code Rules, 2021). It's also required of intermediaries to notify the CERT- In of cybersecurity incidents.

Other laws that contain cybersecurity- related provisions include the Indian Penal Code 1860, which punishes offences committed in cyberspace (such as defamation, cheating, criminal intimidation and profanity), and the Companies Rules 2014 which require companies to ensure that electronic records and systems are secure from unauthorized access and tampering. There are also sector-specific rules issued by regulators and agencies, including the Reserve Bank of India, the Insurance Regulatory and Development Authority of India, the Department of Telecommunications, the Securities Exchange Board of India, the National Health Authority of India, among others, which mandate cybersecurity norms to be maintained by their regulated entities. Cybersecurity of critical information infrastructure – defined as any computer resource that can have a debilitating impact on national security, the economy, public health or safety if incapacitated or destroyed – is regulated by guidelines issued by the National Critical Information Infrastructure Protection Centre[2].

Reporting of Cyber Incidents According to the 2013 regulations, organizations must notify the CERT- In of incidents as soon as possible. Denial of service attacks, phishing and ransomware incidents, website vandalization, and focused network or website scanning are examples of incidents. The 2013 regulations were modified by a new directive issued by CERT- In in April 2022. These modifications included the need to report cybersecurity incidents within six hours, synchronize system clocks with government servers' times, keep security logs in India, and store extra client data. As part of their duties to exercise due diligence, intermediaries are also required by the IT Rules 2021 to report security breaches to the CERT- In. There are also a number of sector-specific reporting requirements. For example, all banks in the financial services industry are obliged to report events as soon as they're discovered, generally within two to six hours. In a similar vein, insurance firms have 48 hours from the time of discovery to notify the Insurance Regulatory and Development Authority of cybersecurity incidents. Telecom license holders must set up a system to keep an eye out for frauds, attacks, and intrusions on their specialized infrastructure and report any similar incidents to the Department of Telecommunication.

[2] Chaudhari, N. (2022, October 19). *Asia Buisness Law Journal*. Retrieved from A comparison of cybersecurity regulations: India: https://law.asia/india-cybersecurity-regulations-2022/