BioSpectrum the business of Bio & Health Sciences

# Why Pharma Industry Must Focus On Cybersecurity?

31 May 2023 | Views | By Kush Kaushik, Co-Founder and Operations Lead, Scrut Automation

**The recent instances of cyberattacks experienced by some of the biggest names in the pharmaceutical industry have raised the alarm concerning the poor state of cybersecurity in the pharmaceutical industry in India. Hence, it is imperative to integrate a more robust cybersecurity infrastructure to support the foundation of the Indian pharmaceutical industry, which is predicted to develop in the coming years.**

The Indian pharmaceutical industry has grown by leaps and bounds in the past decade. The steady functioning of the large end-to-end network is governed by reliable data, which correctly reflects market requirements, both domestically and globally.

Today, data, as the guiding light of the Indian pharmaceutical industry, demands to be protected and secured. However, the recent instances of cyberattacks experienced by some of the biggest names in the pharmaceutical industry, including Sun Pharma (hit by ALPHV Ransomware Group), All India Institutes of Medical Sciences (AIIMS) and Safdarjung Hospital, have raised the alarm concerning the poor state of cybersecurity in the pharmaceutical industry in India. Against the backdrop of the recent security breaches, the need for a robust cybersecurity infrastructure in the pharmaceutical industry has drawn the spotlight towards itself.

**Need for Cybersecurity**

As per data published by CyberPeace Foundation and Autobot Infosec Private Limited, the healthcare industry in India has been victim to 1.9 million cyberattacks till November 28, 2022. Sensitive information, including information on patented drugs,

advances, technologies and even sensitive patient information, might be weaponised by the attackers, eroding customer trust and brand goodwill as a consequence.

The need for a cybersecurity upgrade in various sections of the pharmaceutical industry is urgent. Fortunately, the stakeholders in the industry have registered the importance of such an upgrade and are rooting towards comprehensive cybersecurity solutions, which are also tailored to their needs. The points below further explain the key factors for the need for urgent cybersecurity upgrades in the pharmaceutical industry:

***Rapid Digitalisation***

Rapid upgrade through digitalisation is the norm in every sector. As the pharma industry keeps pace with emerging technologies like the Internet of Things (IoT), big data, cloud computing, artificial intelligence, machine learning, and blockchain, it faces new cybersecurity risks. Although these technologies hold considerable advantages, it's vital for pharma companies to take into account their cybersecurity implications and implement suitable measures to mitigate potential risks.

***Increasing Awareness***

With the growing number of high-profile cyber attacks, the importance of cybersecurity is becoming increasingly evident to businesses in India. As a result, more companies recognise the need to invest in cybersecurity solutions to protect their assets and reputation. One of the best ways to bolster an organisation's cybersecurity posture is via effective employee awareness and training programmes. Attackers frequently use phishing and social engineering tactics to exploit employees and gain unauthorised access to systems. Educating employees on cybersecurity best practices, including creating robust passwords, identifying suspicious emails, and reporting incidents promptly, is therefore crucial.

***Rising Cyber Threats***

The pharmaceutical industry is greatly prone to cyberattacks owing to its ownership of sensitive and valuable data, including data on clinical trials, research and development data, patents and intellectual properties. It also faces a range of cybersecurity threats, including ransomware attacks, phishing scams, malware infections, social engineering tactics, insider threats, and supply chain attacks. These attacks can result in data breaches, system downtime, critical data loss, and damage to the company's reputation. Thus, investment in securing the cybersecurity ecosystem is the need of the hour.

***Regulatory Requirements***

The Indian healthcare industry is subjected to many regulatory requirements, which mandate implementing robust cybersecurity measures to protect personal data. In response to the rising cybersecurity challenges, the Indian government has introduced several cybersecurity regulations, including the National Cyber Security Policy, the Data Protection Bill, and the General Data Protection Regulation. These regulations set rigorous cybersecurity requirements and standards that companies must comply with to enhance their cybersecurity posture and avoid severe penalties.

**Cybersecurity Measures: The Way Forward**

While it is encouraging to see more companies in the pharmaceutical industry recognising the need for investment in cybersecurity solutions, a proactive approach is necessary. Collaborating with cybersecurity experts can help create and implement a comprehensive cybersecurity roadmap that mitigates potential risks, including financial losses, reputational damage, and legal penalties. Major industry players can also actively invest in preventive measures like multi-factor authentication, firewalls, and intrusion detection systems to create an impenetrable cybersecurity ecosystem. While multi-factor authentication requires multiple forms of identification for system access to reduce the risk of fraudulent activities, firewalls and intrusion detection systems are deployed to regulate network traffic, detect unusual activities, and alert administrators against potential cyberattacks and unauthorised access.

Adopting a zero-trust approach and developing a clear roadmap (which around 70 per cent of pharma companies have used to get results in the next two years) is another method to secure data, networks, and access. This approach considers all

users, devices, and applications as potential threats until proven otherwise, necessitating continuous monitoring and logging of all network activity. Pharma companies can also implement robust third-party risk management programmes that meet appropriate cybersecurity standards to minimise the risk associated with third-party vendors with access to sensitive data and systems. Effective incident response and business continuity plans are also essential to mitigate the impact of potential cyberattacks and ensure critical business functions can continue.

Pharma companies can even incorporate effective incident response and business continuity plans to mitigate an attack's impact. These plans should encompass procedures for detecting, containing, and remedying incidents, ensuring that critical business functions can continue even in the event of a disruption. Lastly, the pharmaceutical industry should recognise the importance of customised cybersecurity solutions tailored to their unique needs.

In conclusion, it is imperative to integrate a more robust cybersecurity infrastructure to support the foundation of the Indian pharmaceutical industry, which is predicted to develop in the coming years.

***Kush Kaushik, Co-Founder and Operations Lead, Scrut Automation***