SCRIP
CITELINE COMMERCIAL

30 Mar 2023 | **Analysis**

Ransomware Attacks: The State Of Play As Indian Firms Mount Defense

by Anju Ghangurde

Pharma continues to be targeted by cyber criminals – the latest being India's top-ranked company, Sun Pharma. Experts highlight some of the key vulnerabilities and why firms need to prioritize cyber resilience.

Ransomware attacks against Indian pharma companies appear to be on the rise, exposing the vulnerability of firms that have failed to anticipate the more sophisticated and intrusive techniques of new-age cyber criminals.

Sun Pharmaceutical Industries Ltd., is the latest target of cyber criminals and weeks after flagging up an "IT [information technology] security incident", India's top-ranked drug maker, signaled that it was hit by a ransomware attack and shared some insights on the breach.

The company indicated that as per its current assessment the incident's effect on its IT systems includes a "breach of certain file systems and the theft of certain company and personal data".

Sun declined to clarify the nature or extent of personal data that may have been breached, or whether it expects to engage with the ransomware group but maintained that as part of containment measures, it had proactively isolated its network and initiated the recovery process.

"As a result of these measures, the company's business operations have been impacted. Consequently, revenues are expected to be reduced in some of our

Beware Bad Actors And Avoid A Cyber Security Shock

08 Mar 2023
Medtech and pharma and businesses can take steps to avoid having to claim on their cyber insurance policies, says Edward Machin of law firm Ropes & Gray.

Read the full article here

businesses," Sun said in a recent filing with the Bombay Stock Exchange.

ALPHV was reported by the local media to be behind the Sun attack, with the ransomware group apparently threatening to leak additional documents, including "some interesting things about research", after sharing vignettes of data samples on its site.

While Sun plans to incur expenses in connection with the incident and the remediation, the firm stated that it is currently unable to determine "other potential adverse impacts of the incident, including but not limited to additional information security incidents, increased costs to maintain insurance coverage, the diversion of management and employee time or the possibility of litigation."

Cyber-attacks on pharma are not uncommon nor particularly new and have derailed operations at several large firms over the years. The NotPetya malware attack that rocked *Merck & Co., Inc.* in 2017 was reported to have affected 30,000 computers at the US company and estimated to have cost it $1.4bn in losses while the Winnti attacks in 2018-19, believed to have a China connection, were targeted at *Bayer AG* and *Roche*, among other companies across sectors. (Also see "*Merck Cyberattack Recovery: Congress Scrutinizes Manufacturing Problems*" - Pink Sheet, 21 Sep, 2017.)

The sharp surge in revenues and the massive stack of sensitive data during the pandemic have only brought renewed focus on the sector by cyber criminals. Ongoing geopolitical tensions have added another dimension to cybersecurity threats.

Building Cyber Resilience Capabilities

It's not known if Sun expects to pay up the ransom and decrypt and recover its data but cyber security experts maintained that ransomware firms typically tend to "honor their commitments" once the amount demanded is secured.

"It's a 'business model' as such or else nobody will consider paying up," the cyber security chief of a frontline Indian IT firm told *Scrip* when asked if cyber criminals could go back on their word and raise the stakes.

While cybercrime and legal experts caution firms against making ransomware ransom payment, pharma industry experts said that sensitivity of the data could potentially require companies to engage with the hackers and there might be "some ransom exchanging hands", but companies understand the lack of sustainability of this approach and will continuously build cyber resilience capabilities.

"Unfortunately for the companies, hacking organizations evolve much faster than cyber security tools do, and so companies will constantly be on their toes to keep their data safe. The Data

Protection Bill [in India] is still in its nascent stage and definitely needs to be beefed up to address this angle," Salil Kallianpur, a former executive vice-president at *GSK* in India, told *Scrip*.

Indian firms such as *Dr. Reddy's Laboratories Ltd.*, *Aarti Drugs Limited* and *Ipca Laboratories Ltd.* have been targeted by cyber criminals over the recent past and experts have warned of significant sector-wide vulnerabilities, including the risks that come with third-party associations. In October 2020, Dr Reddy's said that an information security incident involved a ransomware attack and that the company had promptly engaged leading outside cybersecurity experts, launched a comprehensive containment and remediation effort and investigation to address the incident. Last year both Aarti Drugs and Ipca were hit by ransomware attacks. (Also see "*Dr Reddy's Takes Action After Cyber-Attack*" - Generics Bulletin, 22 Oct, 2020.) (Also see "*Cyberattacked Dr. Reddy's Keeps Eye On Sputnik Plans*" - Scrip, 30 Oct, 2020.)

Locked And Bolted: How To Create A Data Fortress

By Jo Shorthouse

11 Nov 2020
Considering the increasing number of biopharmaceutical companies pursuing more virtual and digital tools, the need for world class digital protection is a pressing challenge. *In Vivo* talks to two cyber security experts about best practice when securing data assets.

Read the full article here

Vulnerability Of Systems

Experts have also underscored the "more sophisticated and indiscriminate" nature of cyber attacks beyond the "smash-and-grab" tactics, adding that it will be crucial for Indian firms across the board to prioritize investments in cybersecurity initiatives, more so in the post-pandemic digitized world.

The scale and intensity of cyber threats is alarming to say the least – in 2021 the *Wall Street Journal* reported *Johnson & Johnson*'s then vice president and chief information security officer, Marene Allison, as saying that the US company sees 15.5 billion cyber incidents each day, though the number that "become attacks and get investigated is much lower".

The cyber security chief quoted previously pointed out that traditionally cyber criminals targeted banks, the financial market and intellectual property (IP) and tried to steal data from corporates and nation-states.

Consequently, these sectors were quick to strengthen their cybersecurity infrastructure, while other industries such as healthcare and pharma which have traditionally not been on the radar of cyber criminals as much, never really prioritized upgrading their infrastructure.

“In the wider Indian pharma industry context, the problem is perhaps much more acute, because organizations have not spent enough money to really create a basic hygiene infrastructure; they tend to use obsolete systems, they don't patch their solutions. So, they are highly vulnerable,” the cyber security head explained.

A report by the Data Security Council of India (DSCI) and Deloitte India earlier noted that legacy systems, third-party risks, data and IP risks, and securing the operational technology (OT) environment are the top challenges that pharma security leaders face in India. Securing OT systems is also a major concern globally for the biopharma sector as firms shift to embrace newer technologies in production and supply.

Raising Cyber Security Investments

But the pandemic has brought cyber security concerns to the fore at least at some frontline Indian firms.

Ex-GSK executive Kallianpur, who now runs a digital health consultancy, noted that cyber-attacks are an unintended consequence of digital transformation and the rising importance of data storage and management.

“As the importance of digital and data became more obvious after 2020, we began to see pharma companies in India significantly increase their investments into cyber security,” Kallianpur stated.

The DSCI-Deloitte report, he added, said that ransomware attacks, IP and data theft have been the top causes of concern for pharma, both in India and globally.

Leading Indian firms are prioritizing protection of data and IP, managing third-party and supply chain risks, planning the retirement of legacy systems, and securing the OT environment. Cybersecurity investments between 2019 and 2021 have increased by a minimum of 25-30 per cent, while in some organizations, it doubled during the pandemic, the report indicated. Cybersecurity is estimated to account for about 5-8 per cent of IT spending in leading pharma companies.

“Cybersecurity is one of the most important enablers of digital transformation and this has led to several top companies adopting, what the report calls, a ‘zero trust approach’ and hence spending more to develop cyber resilience,” Kallianpur added.

Sharing Intelligence And Best Practices

Experts in India are also calling for greater cohesive stakeholder efforts and board level engagement in companies, to fortify the cyber security ecosystem.

Kallianpur noted that post the recent cyber attacks against Ipca and other Indian firms, cyber experts acknowledged that most Indian healthcare and pharmaceutical companies lack basic cybersecurity practices in place. Many of them depend on government insights to fight cyberattacks, he maintained.

"A lot more thinking and deliberations are needed in India pharma boardrooms to create an exhaustive strategy on how companies should deal with ransom demands, keeping data safe and building cybersecurity features for the future," the executive said.

The DSCI-Deloitte report, among a string of recommendations, suggested that nodal bodies, such as Computer Emergency Response Team (CERT) should engage with pharma chief information security officers for intelligence and best practices sharing.

The cyber security expert quoted previously noted that most of the advisories of the Indian Computer Emergency Response Team (CERT-In) will likely be applicable to pharmaceutical companies but also called for greater collaboration on information sharing and communication on cyber security matters among stakeholders. CERT-In, whose objective is to secure the Indian cyber space, is the national nodal agency for responding to computer security incidents as and when they occur.

Internationally, organizations like the non-profit Health-ISAC Inc (Health Information Sharing and Analysis Center), provides healthcare stakeholders a forum for co-ordinating, collaborating and sharing vital physical and cyber threat intelligence and best practices with one another.