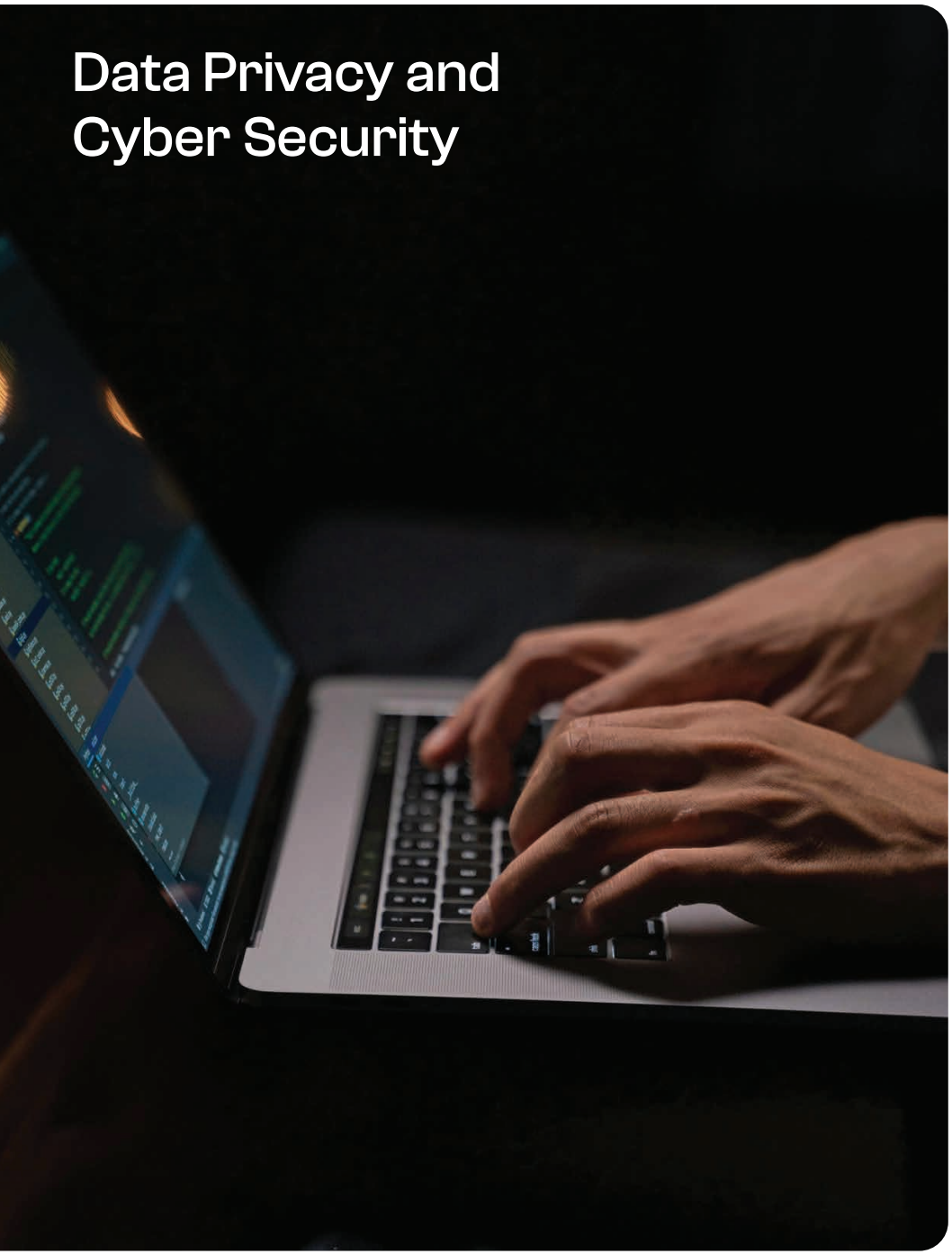
Data Privacy and Cyber Security



Context

Recently, the pharmaceutical industry experienced a considerable functional shift with hybrid work, digital workplaces, and other trends. Further, automation and digitalization are becoming significant parts of R&D, manufacturing, and supply chain management,[15] inevitably creating a need for focused cyber-attack prevention, In our industry, intellectual property loss and operational disruptions are the two most significant cybersecurity risks resulting in reputation damage. Such incidents lead to severe compliance breaches as health-sensitive data is involved.[16] In 2022 alone (until the 28th of November), there were 1.9 million cyberattacks on India's healthcare sector.[17] Unpatched vulnerabilities and fundamental misconfigurations were responsible mostly, mandating a new security approach with a dedicated vulnerability management strategy.[18]

Approach

Our IT initiatives are guided by our Information Security Management System, which provides a framework for managing IT operations. We employ robust, multi-layered data privacy and security systems, including advanced encryption, secure access controls, and regular audits to ensure data integrity and confidentiality. We follow strict protocols for data handling, storage, and disposal meeting regulatory requirements, and offering comprehensive employee training and awareness programs.

We are strengthening data security and making structural changes to our operations. Notably, our API facilities are undergoing a digital transformation, allowing finance, marketing, production, and supply chain teams to use a unified data platform for improved information transparency.

Actions & Initiatives

Information Security

We maintain 24/7 security and network operation centers that quickly isolate systems affected by cyber-attacks, managed by an external third party. To reduce cyber threat risks, we use micro-segmentation for tailored security measures and conduct Vulnerability Assessment and Penetration Testing (VAPT) to identify vulnerabilities. Our endpoint detection and response (EDR) tool allows for rapid threat neutralization at endpoints, and we employ multiple firewalls, ensuring they are regularly updated for enhanced security.

[15] https://www2.deloitte.com/in/en/pages/risk/articles/Indian-pharma-takes-the-digital-leap.html
[16] https://www.pharmaceutical-technology.com/comment/cybersecurity-in-pharma-qa-with-globaldata-thematic-analyst/
[17] https://www.livemint.com/technology/tech-news/indian-healthcare-sector-suffers-1-9-million-cyberattacks-in-2022-11669878864152.html
[18] https://www.businesstoday.in/industry/pharma/story/indias-pharma-firms-need-strong-cyber-defenses-says-cybersecurity-expert-389514-2023-07-13

We regularly update our IT Policy procedures, fully automate data backups, and enhance storage capabilities. We are implementing cloud backup for critical applications and establishing disaster recovery sites for essential systems, having also conducted a third-party gap assessment for GxP systems per 21 CFR Part 11. Additionally, we have increased cybersecurity and information security awareness sessions for employees, including exams and certifications, and conducted phishing simulations to assess responses to fraudulent emails.

During the reporting period, we faced a ransomware attack impacting certain IT assets. While a group claimed responsibility, we regard it as a grave concern. Our response involved a significant effort to address regulatory standards, achieve recertifications, and system enhancements. We strengthened our cybersecurity by establishing a 24/7 Security Operations Center (SOC), implementing micro-segmentation, deploying advanced spam filters, and improving endpoint detection and response. We also enhanced vulnerability assessments and configured Data Loss Prevention (DLP) systems to mitigate data loss risks. All employees receive regular training on cybersecurity, data protection, and privacy.

24/7

Security Operation Center

Green Practices

We have refined our device-sourcing procedures to ensure all devices have green certifications and reduce our overall device consumption. While we monitor printer paper usage, some departments still print for legal reasons, resulting in about 250,000 printouts monthly. Electronic waste disposal is handled by a certified third-party vendor.

Outlook

Each year, we aim to significantly enhance our data security practices, targeting zero data privacy and cybersecurity breaches. To achieve this, we will conduct a third-party vulnerability assessment and evaluate IT and OT security gaps. We also plan to implement an annual cyber safety training program for specific Granules staff to ensure full participation. As part of our digital transformation, we are adopting innovative methods that are already yielding positive results. Following a thorough assessment of our operational technology systems, we aim to achieve ISO 27001 certification by the end of 2024.