Deloitte.

DSCI
PROMOTING DATA PROTECTION

Indian pharma takes the digital leap

What does it mean for cybersecurity?

June 2022

Contents

Foreword

The Indian pharma sector came centre stage during the pandemic, for developing a home-grown vaccine in record time and for being a key supplier of essential vaccines and drugs to the world. Total pharma exports in FY2021 stood at US$24.35 billion, with a trade surplus of US$17.68 billion.[1] India happens to be the leading supplier of generic medicines, holding 20 percent share in global supply (by volume).[2] The government through its Production Linked Incentive (PLI) schemes is encouraging production of not only Active Pharmaceutical Ingredients (API) and drug intermediaries, but also biopharmaceuticals, complex generics, and repurposed drugs.[3] All these indicate the depth and breadth of scale that the Indian pharma Industry is aiming to achieve. It is a great opportunity for Indian pharma sector to become one of the leading global suppliers of high-end innovative drugs by leveraging its R&D and low-cost production in the country. At the same time, organisations can also leverage the rapidly evolving health care landscape in India to offer innovative digital solutions and personalised care.

To understand the pulse and priorities of the sector (from a business, digital, and cybersecurity standpoint), Data Security Council of India (DSCI) and Deloitte India conducted discussions with large pharma companies and industry experts in India and globally. It has been extremely encouraging to see that the sector is charged up to capitalise on the next phase of growth, driven by digital transformation, with a strong focus on smart manufacturing, digital supply chain, and customer value proposition. There is a palpable adoption of cloud by leading pharma firms, with a 20 percent increase in cloud workloads in the past two years. With a strong focus on cloud, automation, and analytics, the sector also wishes to leverage Artificial Intelligence (AI)/Machine Learning (ML) across the value chain, from improving drug discovery in R&D to predictive maintenance and streamlining of processes in manufacturing.

Amidst this transformation, and to an extent propelled by the pandemic, it is important to note that cybersecurity considerations have taken a centre stage. The leading pharma firms in India are prioritising protection of data and Intellectual Property (IP), managing third-party and supply chain risks, planning the retirement of legacy systems, and securing the Operational Technology (OT) environment. Cybersecurity investments between 2019 and 2021, have increased by a minimum of 25-30 percent; while in some organisations, it has doubled during the pandemic. Key areas of investments in large pharma firms have been security assessments, attack surface management, next-gen Security Operations Centre (SOC), managed threat intelligence, and data security. There is an increasing focus on solutions, such as next-gen End-point Detection and Response (EDR), digital identity, and User and Entity Behavior Analytics (UEBA). Ransomware attacks, IP and data theft have been the top causes of worry for the sector, both in India and globally. Leading pharma companies are also looking at a roadmap to adopt zero trust security in the next couple of years. For organisations that have made significant investments in the past two years, the future roadmap will entail enhanced monitoring, cost optimisation through automation and outsourcing, and cybersecurity with regards to digital transformation. A robust OT security strategy, and a constant endeavour to plug security leaks in the supply chain, will continue to hold strong focus.

Source: 1. Government of India, Ministry of Chemicals & Fertilizers, Department of Pharmaceutical - Annual Report 2021-22; 2. Invest India; 3. Press Information Bureau, Government of India

Foreword

The nature of the pharma ecosystem is quite diverse and fragmented, which has a large ecosystem of Micro, Small and Medium Enterprises (MSMEs) that address niche areas within the value chain. Such a diverse base requires cyber and privacy awareness across all organisations of various sizes. The PLI schemes and support from the government will encourage more niche manufacturers and research-led organisations to expand their capacity and footprint, working closely with leading pharma companies. To enable a robust and secure collaborative environment, it is imperative that MSMEs and other pharma organisations also adopt baseline security measures and hygiene.

Through this report, we aim to bring out the rapid changes that the pharma sector is witnessing, supported by digital transformation, and the way it affects their cybersecurity posture. The report goes into the facets of digital and cybersecurity priorities of leading pharma organisations, with a spotlight on best practices. It is further aimed at catalysing discussions to bolster the security posture of the entire ecosystem, with a focus on the MSME sector.

We would like to express our gratitude to the industry experts who have contributed to the report, through their valuable time and insights. We hope you find the report useful, and it helps you in your cyber security roadmap and readiness.

Rama Vedashree
CEO, DSCI

Gaurav Shukla
Partner and Leader, Cyber, Risk Advisory, Deloitte India

Jaishil Shah
Partner, Risk Advisory, Deloitte India

Executive summary

Market and business

A fragmented, yet vibrant pharma landscape

- Total India pharma market (domestic + exports) at more than US$45 billion; expected to become **US$120 -130 billion by 2030**
- Strong government support through **PLI schemes**
- Recently, India started the manufacturing of 35 APIs that were not manufactured before
- Rising focus on specialty pharma and R&D
- Key challenges – The United States Food and Drug Administration (US FDA) scrutiny on manufacturing sites, generic pricing pressure, and supply-chain challenges

Digital

Current priorities – Digital transformation across manufacturing, launch/commercialisation, and supply chain

— **Manufacturing** – Data digitisation, analytics, dashboarding, industrial automation, industrial IoT, remote audits and operations

— **Supply chain** – Digital supply chain with end-to-end visibility, supplier marketplace, data-driven insights for demand management, track and trace, automation

— **Launch and commercialisation** – Virtual medical detailing, disease monitoring and management platform, health care service platform, awareness and education platforms

— **R&D** – Information management tools, collaborative tools, automation, data lake and analytics, AI in pre-clinical research for ligand identification

- Rising focus on **cloud, automation, data analytics, and AI/ML**
- On an average, 20 percent increase in cloud workload in the past two years; focus on Good Practices **(GxP)**, data security, and GDPR compliance

Cybersecurity

How did the pandemic increase security requirements?

Need for remote operations and remote collaborations at scale, rise in end-points, third-party software and cloud, opening the OT environment

Cybersecurity concerns and priorities

- Top cybersecurity concerns – Protecting data and IP, third-party and supply-chain risks, legacy systems, and securing the OT environment
- Moderate concerns – Securing remote access, cloud security, stakeholder and employee awareness, and cyber talent management
- Cybersecurity as a percent of IT investment – 5 – 8 percent
- 70 percent have a focus on zero trust security
- 55 percent have a hybrid SOC; key areas of interest - Managed Detect and Response (MDR), more coverage of end-points, Security Orchestration, Automation And Response (SOAR), user-entity and behavioural analytics, breach and attack simulation
- Real-time threat intel, threat hunting, and dark web monitoring are garnering interest

Cybersecurity governance

- Cybersecurity function mapped to IT function
- Privacy governance still evolving with current mapping with the security function

Methodology

Study methodology

DSCI and Deloitte conducted more than 25 expert discussions between August 2021 and March 2022, where leading pharma companies and industry experts in India and globally shared their views on the pulse of the sector and the rising focus on cybersecurity.

Scope

Leading pharma companies (with revenues > INR 3,000 crore)

Desk research

In-depth secondary research

To gather information, develop preliminary understanding, and design a questionnaire for expert/industry consultations

Data sources:

- Market reports
- Company annual reports
- Press releases, media bytes
- Industry association coverage
- Analyst coverage
- Government websites

Expert discussions

More than 10 discussions with global and Indian pharma industry experts (internal Deloitte and DSCI experts and external industry experts)

To develop robust understanding, gather information, and validate findings on pharma industry trends, digitalisation, and cybersecurity environment

Industry consultations

More than 15 discussions with CIOs/CISOs of prominent pharma companies in India

To aggregate insights, challenges, best practices, and outlook

Analysis and report development

Data consolidation, analysis, and report writing

Output

- The report encapsulates our learning on market developments, digital transformation, and the impact on cybersecurity requirements, **as seen in the leading pharma companies in India.**
- It aims to present digital and cybersecurity priorities in these companies, with a spotlight on both Indian and global best practices.

Global perspective

Global pharma sector trends in 2021 – Accelerating industry change

The pandemic placed an enormous strain on the pharma sector's workforce, infrastructure, and supply chain. In spite of that, it also accelerated digital transformation to bolster the value chain, focus on innovation and productivity, and patient experience.

Digital transformation

Digital enterprise

- End-to-end transformation across the value chain
- From doing digital to being digital
- Intelligent optimisation (intelligent workflow and human-machine decision making)
- Strong focus on high-quality data and analytics
- AI across the value chain

Manufacturing and supply chain

- Smart and sustainable factories
- Minimising cyber risks in manufacturing and supply chain
- Building supply chain resilience – End-to-end visibility enabled by technology, thorough risk assessment, and regionalising supply of critical materials
- Digital innovations – Building control towers or data-hubs integrating internal and partner data, AI-enabled forecasting, root-cause analysis, and enhanced track and trace using AI, IoT, blockchain

Regulatory transformation

Agile and collaborative regulatory environment Approval timelines reduced from 10 years to 10 months (rolling submissions for a shorter timeline, automating processes)

- Regulators' global cooperation and collaboration
- Rise in digital and virtual, such as for document sharing and facility tours/inspection

Workforce experience

Workforce experience and talent development

- Agile work environment; less hierarchy more networked
- Diverse mix of external resources and gig workers
- From digital workplace to virtual office
- More focus on culture and collaboration
- Upskilling of employees' digital and data skills

Patient experience

Transforming patient experience

- Co-creating with patients; personalised experience and therapies
- AI-driven engagement; connected patient and physician platforms
- Digital, a key priority – Digital health to digital therapeutics
- Digital connected health ecosystems that enable real-time data and analytics and serve as centres for education, prevention, and treatment

R&D and collaboration

Focus on R&D productivity and industry collaboration

- Rising RoI on innovation, supported by COVID-19 portfolio, and emergency approvals
- R&D future labs (interconnected ecosystem, supported by data, digital platforms, and analytics)
- New-age clinical trials (rapid digitisation with telemedicine, IoT, and wearable device; decentralisation of trials through remote enablement; digital is enabling real-world evidence)
- Unprecedented collaboration for research

Source: Deloitte 2022 Global Life Sciences Outlook

Key cyber threats confronting the pharma sector

Amidst this transformation and digitalisation journey, pharma companies are being targeted mainly for the data and core technology. In this age of rising geopolitical tensions, stalling of operations is also a big motive for the state-sponsored attack groups. Threats from third-party network or software, threats to new-age technologies (automation and AI), threats to the vulnerable OT systems, and ransomware threats keep the security teams worried. As digital adoption and innovation continue to drive competitive advantage for pharma companies, the sector will continue to be in the radar of threat actors (state or non-state).

Manufacturing threats

Nation-state Advanced Persistent Threat (APT) group's motivations for targeting of manufacturing and supply chain environments may be to exfiltrate proprietary data on medical innovations to benefit their domestic businesses or could be associated with broader requirements from national intelligence groups. It is not just about data theft, rising IT-OT integration in the factory floor can let any malware make its way to the OT systems, with the potential to stall operations, and jeopardise the supply of critical drugs/vaccines. According to a 2021 survey by Fortinet[1] (with professionals involved in OT security), 45 percent respondents highlighted IT-OT convergence as a key impact to overall security posture of an organisation.

Data breaches, IP theft (vaccine espionage)

IP data is highly valued by both cybercriminals and APT actors, resulting in pharma organisations becoming prime targets for data theft. In May 2020, the US Government issued a warning against state-sponsored groups trying to access research-related information from entities involved in COVID-19 vaccine research.[2]

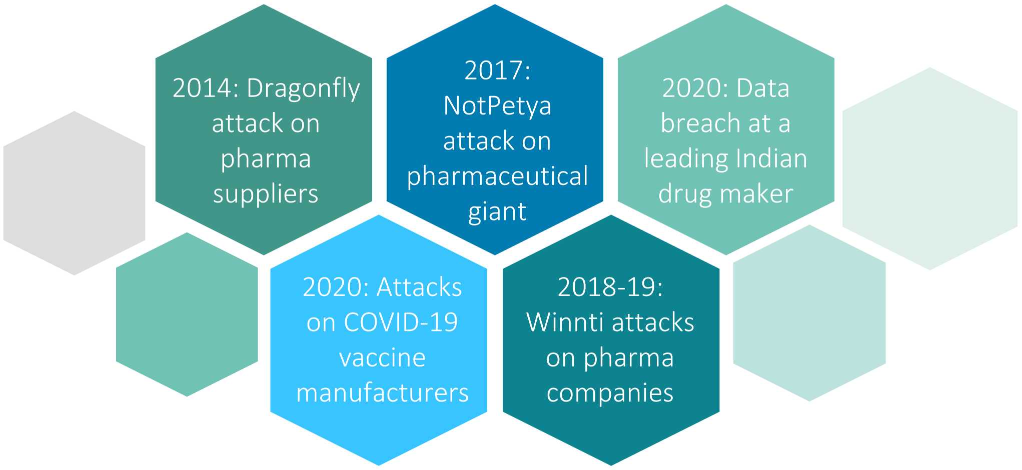
Cross-industry threats

Pharma organisations continue to face cross-industry threats (commonly observed across various industries), which includes supply chain attacks, threats to enterprise resource planning systems, threats from M&As, compromised third-party network, threats to enterprise mobile devices, ransomware threats, Business Email Compromise (BEC), remote access trojans, and information stealing malware.

APT targeting pharma organisations

Targeting the IP of pharmaceutical organistaions (R&D, formulations, and manufacturing data) by nation-state backed APT groups, is a key concern area. The theft of proprietary business processes, innovative technologies, customer data, and other IP from pharma organisations can support domestic businesses and provide a competitive advantage to nation states in competing markets.

Pharma cybersecurity breaches identified in the past



2014: Dragonfly attack on pharma suppliers

2017: NotPetya attack on pharmaceutical giant

2020: Data breach at a leading Indian drug maker

2020: Attacks on COVID-19 vaccine manufacturers

2018-19: Winnti attacks on pharma companies

Source: 1. Fortinet The 2021 State of Pharmaceuticals and Cybersecurity Report; 2. NBC News

Key regulations – Cybersecurity, privacy, and good practices (GxP)

Given below are some of the key regulations (not limited to) that impact pharma companies. Further to this, every country has its own set of local security and privacy laws that organisations doing business in such geographies must comply (example, China Personal Information Protection Law [PIPL] and Brazil General Data Protection Law [LGPD] etc.)

GxP and data integrity

US FDA 21 CFR Part 11 – 2003[1]

FDA's regulation on electronic records and signatures, to protect integrity of data and systems, involved in FDA submissions

New EU Annex 11 – 2011[2]

Guidelines for the use of computerised systems in GMP regulated activities to ensure product quality, safety, and efficacy

Data protection

European General Data Protection Regulation (EU GDPR) – 2016[3]

The General Data Protection Regulation 2016/679 is an EU law covering data protection and privacy in the European Economic Area (EEA), which includes all EU countries along with Iceland, Liechtenstein and Norway. Transfer of personal data outside the EEA is also included.

Draft Data Protection Bill (India) – 2021

The Draft Data Protection Bill 2021 was finalised by the Joint Parliamentary Committee[4], which is expected to bring a data protection legislation in India and impact the way businesses handle data.

Risk management and incident reporting

SEC's new cybersecurity proposal – 2022[5]

U.S. Securities and Exchange Commission's (SEC) new cybersecurity proposal for public companies covers cyber risk management, strategy, governance, and incident reporting. It calls for disclosing material security incidents within four business days.

CERT-In directions (India) – 2022[6]

Calls for reporting cyber incidents to Indian Computer Emergency Response Team (CERT-In) within six hours of detection. Cyber incidents across 20 categories are listed, which includes targeted probing of critical networks/systems, unauthorised access, and identity theft.

Source: 1. FDA Guidance for Industry; 2. EudraLex Volume 4, Annex 11; 3. EU GDPR; 4. Parliament of India – Lok Sabha; 5. SEC; 6. CERT-In

India perspective

Digital Transformation

Indian pharma – A vibrant landscape

India's pharma prowess had been known for a very long time, particularly it's contribution to the world in fighting the AIDS epidemic. According to the 'Annual Report - 2020-2021' by Government of India[1], India's contribution stands at 60 percent in global vaccine production and for measles vaccine, India fulfils 90 percent of World Health Organisation's (WHO) demand. India is known as the largest supplier of generic medicines, contributing about 20 percent to the global supply (by volume), also with the highest number of US-FDA approved manufacturing sites outside the US. Additionally, India rose to eminence after developing COVID-19 vaccine in record time, and after supplying essential vaccines and drugs to the world, during the pandemic. It became evident that India is poised to take up the title of 'the pharmacy of the world'.

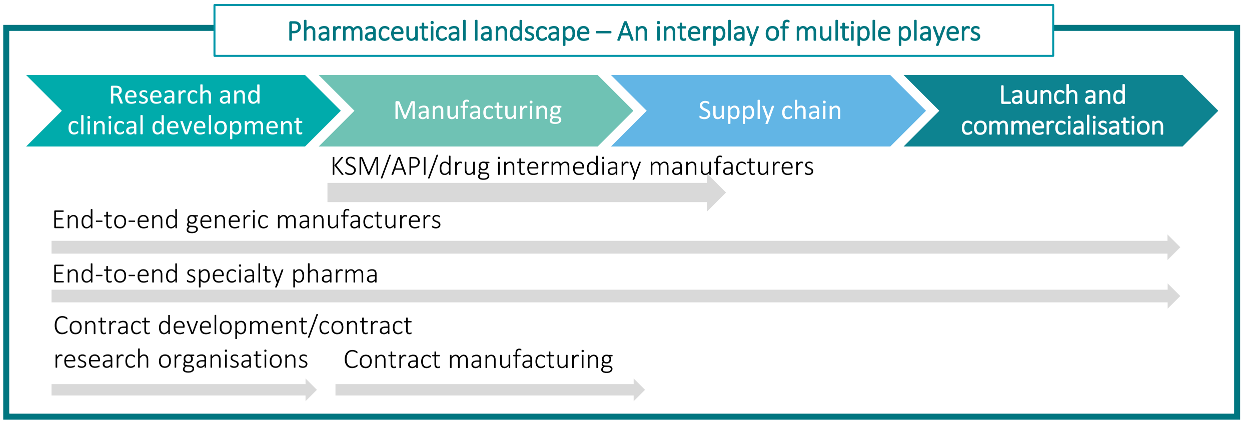
According to Invest India[2], the pharmaceutical market in India is poised to reach US$120-130 billion by 2030. The domestic spending grew at a CAGR of 9.5 percent, from 2016 to 2020 to reach US$21 billion in 2020[3]. Total pharma exports stood at US$24.35 billion in FY2021[1], bringing the total current size of pharma market to more than US$45 billion.

To boost the sector and reduce global dependencies, the Indian Government also released two batches of incentive schemes - PLI 1.0[2] worth INR6,940 crore for bulk drug manufacturing, and PLI 2.0[4] worth INR15,000 crore for manufacturing of various product categories, such as biopharmaceuticals, complex generics, API/Key Starting Material (KSM)/drug intermediaries, and repurposed drugs. With regards to foreign investments in pharma[2], 100 percent FDI is allowed for greenfield projects via automatic route and for brownfield projects, where 74 percent is allowed via automatic route and rest via government approval. In FY2021, FDI in pharma sector saw a 200 percent increase[5] from the previous year. All of these indicate the vibrancy of the India pharma market, which is steadily making a transition plan towards innovative product portfolio.

India's pharmaceutical landscape is quite diverse, with expertise in both small molecule and large molecule development. There are organisations that function end-to-end across the pharma value chain, while others play only in specific segments. India's pharma landscape is highly fragmented, but from a revenue distribution standpoint the top 30 pharma companies contribute roughly 70% of the total market[6].

The COVID-19 pandemic has put the necessary spotlight on the Indian pharma sector, prompting it to contribute to the country and the world. India has a prominent role to play in high-end generic manufacturing. The low-cost manufacturing abilities can improve accessibility of medicines. But in the post-pandemic world, the real differentiator will be Indian pharma's ascension to becoming innovators, by creating innovative drugs, digital solutions, personalised health care, thus, enhancing quality, accessibility, and affordability across the care pathway. Meanwhile, the pharma sector will also have to find a way to enhance manufacturing efficiencies, optimise the supply chain, with a strong focus on good manufacturing and distribution practices.

> One of the key enablers to achieve all this is through DIGITAL.


Pharmaceutical landscape – An interplay of multiple players

Research and clinical development

Manufacturing

Supply chain

Launch and commercialisation

KSM/API/drug intermediary manufacturers

End-to-end generic manufacturers

End-to-end specialty pharma

Contract development/contract research organisations

Contract manufacturing

Source: 1. Government of India, Ministry of Chemicals & Fertilizers, Department of Pharmaceutical - Annual Report 2021-22; 2. Invest India; 3. Pharma Company Annual Report; 4. Press Information Bureau, Government of India; 5. Mint; 6. DSCI-Deloitte analysis

Digital transformation in the Indian pharma sector

Evolution of digitalisation in the leading pharma companies

2015 onwards

2015 was the era of third-party software, such as Laboratory Information Management System (LIMS), quality management solutions, and data document management solutions.

2018 and onwards

2018 saw increased focus on automating factory floors; more digital initiatives for customer outreach; and an overall rise in the willingness to explore data-driven insights across functions, leveraging data warehouse, data lake, big data, and enhanced data visualisation.

Pandemic and after

The pandemic catapulted the focus on remote audit, enablement, and execution of processes with regards to manufacturing; compliance check of digital systems; use of analytics and AI; remote desktops; Industry 4.0; digital supply chain; and a commitment towards cloud.

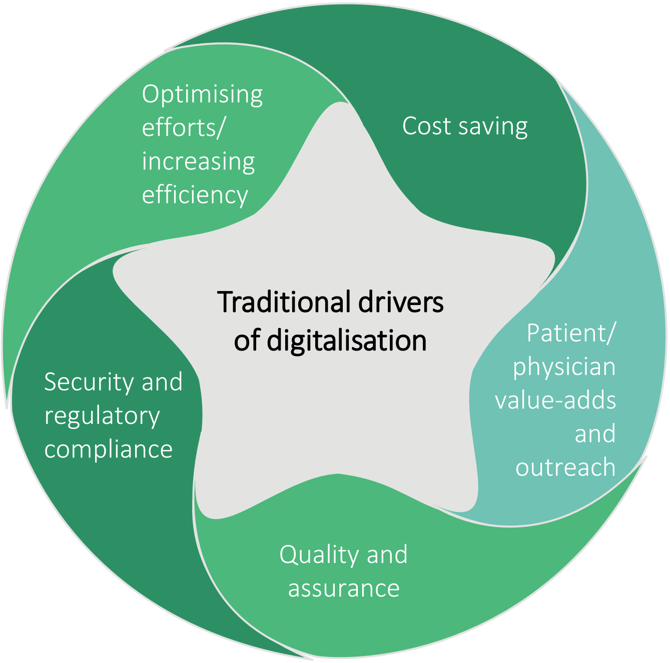
It is interesting to note that the leading pharma companies in India had undertaken their digital journeys before 2015. The overall willingness to harness the true potential of digital transformation became prominent around 2017/2018, followed by the pandemic which provided the rest of the impetus.

While optimisation of processes, cost saving, and regulatory push have been the key drivers for digital transformation traditionally, the pandemic also brought in the need for remote working capabilities.

The corporate side of the pharma (which includes functions such as finance, HR, sales, and marketing) is witnessing changes like any other sector with hybrid work models, digital workplace, use of collaboration tools, digital learning, digital recruitment, etc. At the same time, it is interesting to note the scope and scale of digitalisation happening across certain key functions of the pharma value chain, including research and clinical development, manufacturing, supply chain, and commercialisation.

Indicative examples of pre-pandemic digitalisation

- According to a 2017 media article, a life sciences company had already digitised 40-50 percent of its processes and was looking to adopt a cloud-first strategy.
- A 2019 news report highlighted one of the leading pharma company’s digitisation journey, with 70 percent paper removal from plants.


Optimising efforts/ increasing efficiency
Cost saving
Traditional drivers of digitalisation
Patient/ physician value-adds and outreach
Security and regulatory compliance
Quality and assurance

Digital transformation across the value chain

Research and clinical development

- Use of LIMS, Electronic Lab Notebook (ELN), and integration with instruments
- Data aggregation and big data/analytics
- AI in pre-clinical ligand identification and other scientific literature review
- Digital collaboration platform
- Drug repurposing
- Clinical trial management systems
- Pharmacovigilance in clinical trials

Manufacturing

- Data digitisation, analytics, dashboarding
- Manufacturing Execution Systems (MES), connecting whole batch, integration of MES with business software
- Industrial automation
- Industrial IoT – Temperature loggers, industrial tablets, WiFi connectivity
- Remote audits and operations

Supply chain

- End-to-end visibility of the supply chain
- Marketplace solutions connecting health care stakeholders, to improve reach and accessibility
- Data-driven insights for stock and demand management; predictive analytics
- Zero trust supply chain cloud for data/knowledge sharing
- Barcoding and tracking; AI, IoT, blockchain for enhanced tracking and tracing
- Automation

Launch and commercialisation

- Virtual medical detailing
- Awareness and education platforms for patients and physicians
- Monitoring and management platforms for diseases
- Health care services platform
- Population health management
- Adverse event reporting
- Sales force and KOL management

- IT implementation by pharma companies in India observe compliance with 21 CFR Part 11[1] of the FDA's regulation on electronic records and signatures. The regulation puts forth both procedural and technical requirements for organisations that have electronic records of data. Such data are important from a quality and safety standpoint and are used in regulatory (FDA) submissions.
- The compliance is meant to protect integrity of data and systems, and correlates to good practices. It applies to research, clinical, and manufacturing environment.
- Key areas of compliance: Validation, audit trail, copies of records, and record retention. Validation includes Installation Qualification (IQ), Operational Qualification (OQ), and Performance Qualification (PQ), and apart from validation of individual software, the entire system and workflow also requires a validation.

Source: 1. FDA Guidance for Industry

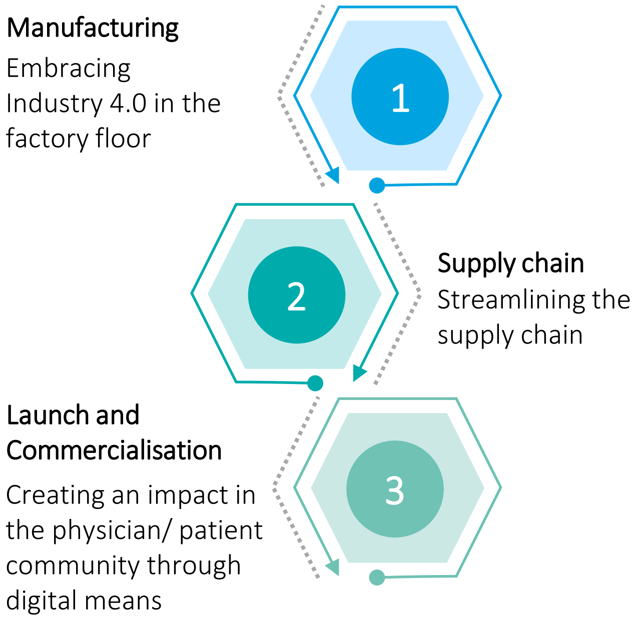
Current priorities for the pharma industry – Digital transformation across manufacturing, outreach, and supply chain

To scale globally at par with the leading innovators of the world, the Indian pharma sector needs to adopt innovative means to streamline processes, cut down costs, and maintain trust in the ecosystem, which digital can deliver. According to Gartner, the second quarter of 2021 witnessed sluggishness with regards to technology spending in India, but certain sectors such as the pharma, health care, and financial services continued to invest in digital transformation.

This is likely to increase as leading traditional pharma companies gear up to become cloud-first and digital-first organisations and enter collaborations and partnerships with technology firms to achieve their goals and aspirations.

Our discussions with industry leaders and CIOs of leading companies in India suggest three key current digitalisation priorities for pharma:

Current digitalisation priorities



Manufacturing
Embracing Industry 4.0 in the factory floor

1

2

Supply chain
Streamlining the supply chain

Launch and Commercialisation
Creating an impact in the physician/ patient community through digital means

3

1

Manufacturing

Embracing Industry 4.0 in the factory floor

Streamlining of manufacturing and supply chain with real-time integration between the two is considered a panacea for pharma companies in India. The pandemic led to an increased focus on automation, industrial IoT, remote audits and enablement, dashboarding, and data-driven insights. This is going to only increase in the future. Leading pharma companies are evaluating creation of digital twin, touch-less factories to maximise efficiencies and minimise loses. As pharma companies in India gear up to embrace Industry 4.0, our research highlights the three pre-requisites:

1. A robust organisational strategy for the transition, and for IT-OT integration
2. A data architecture/infrastructure strategy to generate the right data and use it at the right time to drive meaningful insights
3. Keeping cybersecurity at the core of such transition

- According to a recent report by NASSCOM[1] on India Industry 4.0 adoption, the pharma sector is believed to be in early or intermediate stages, with a focus on cloud-based adoption.
- It is interesting to note that the sector had the second highest Return on Invested Capital (RoIC) of 16 percent as of FY2019, which is a good indicator for adoption.

Source: 1. NASSCOM report - India Industry 4.0 Adoption: A Case to Mature Manufacturing Digitalization by 2025

2

Streamlining the supply chain

Supply chain improvement (both upstream and downstream supply chains) is one of the key requisites for pharma companies to ensure quality and availability and minimise losses. Also, the challenge of counterfeit drugs, which accounts for 10.5 percent[1] of drugs sold in low and middle-income countries, necessitates the use of technology to be able to counter it. Research by Digital Supply Chain Institute[2] highlights that digitising the supply chain has the potential to increase revenue by 10 percent across sectors. The pandemic brought in significant focus on supply chain security – the need to diversify risks, improve track and trace, and optimise the whole process, from procurement and manufacturing to supply and distribution.

Key focus areas for digital transformation of the supply chain are:

1. End-to-end visibility of the supply chain
2. Cloud-based connected supplier platform
3. Analytics and insights for increasing efficiency, for inventory management, and managing demand and supply
4. Barcoding, AI, IoT, and blockchain for enhanced track and trace, to prevent delays, wastages, pilferage, and counterfeiting
5. Connectivity and interoperability with other business software

With integration and data sharing with several third-party organisations, it is also crucial to have a third-party risk management process in place. It is important to conduct adequate due diligence, ensure compliance checks, and stay committed towards cybersecurity, data protection, and privacy to prevent any possible breach in the value chain.

Source: 1. Mint; 2. Digital Supply Chains: A Frontside Flip – Report by Digital Supply Chain Institute

Case Study

Procurement

- It is observed that leading Indian pharma companies use various software to streamline their procurement processes.
- A leading pharma company is believed to have saved US$6,00,000 within the first six months of using one such solution.
- Another leading Indian pharma company has its own portal for its business partners to simplify partner connect and purchases.

Source: Media articles

Case Study

Supply

Several key Indian pharma companies are investing in a new venture for better goods distribution.

This new entity proposed to acquire a B2B health care platform, which would offer the following:

1. Supplier marketplace
2. End-to-end supply-chain visibility
3. Insights on stock availability, schemes, etc.
4. Masking sensitive information and providing only aggregated insights
5. Interoperability with business software

Source: Media articles

3

Launch and Commercialisation

Adopting innovative means to create an impact in the physician/patient community

Indian pharma companies are following the global trend of adopting digital initiatives to create better value propositions for physicians, patients, and other health care stakeholders. Pharma companies no longer wish to be just drug makers but want to create an impact across the health care value chain from awareness and diagnosis to disease monitoring and management.

Newer business initiatives and models are emerging for exploring the space of digital health and therapeutics, through in-house initiatives, subsidiaries, collaborations, and investments.

Indicative examples

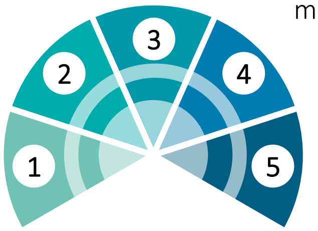
A leading pharma company incorporates a wholly owned subsidiary to explore the digital health care space aimed at creating platforms for patients and physicians.

A **leading pharma company** floats a wholly owned arm, with an objective to bring together various health care services (doctors, labs, insurance, etc.) on a common platform and provide a comprehensive experience

A **leading pharma company** invests in a diabetes management platform

A **leading biopharma company** collaborates with a digital therapeutics company to offer solutions for better management of diabetes (including automated dose recommendations, remote monitoring, etc.)

A **global pharma company** launches a platform for education and adherence to medicine


Health care services platforms
Continued medical education for physicians
Disease monitoring and management
Awareness and education
Adherence
1
2
3
4
5

Digital health programmes aimed at empowering health stakeholders

The digital health programmes by pharma companies not only improve the engagement of physicians and patients but the data, analytics, and insights can pave a way for personalised care and medicine, and there is an interest in exploring AI/ML solutions for such purposes.

The digital health entities and startups that collaborate with pharma companies are either digital natives or well equipped to bring in the expertise of handling data and information with utmost care (compliant with global guidelines such as GDPR).

Source: Media articles

While innovation around outreach existed before, the pandemic accelerated focus on empowering physicians and patients to enable and enhance care-giving from home.

The next frontier for digital is research and clinical development

Pharma firms in the US are leveraging disruptive technologies and digital tools for various R&D activities, such as target identification/validation, lead identification, and use of AI models; and for clinical trial activities such as trial design, patient recruitment, predicting outcomes, and analysis. From a digital standpoint, R&D is such a big focus area globally that experts highlight 'Shadow IT' becoming a challenge within the R&D set-up. However, in India, while there is awareness around the benefits of digital solutions within R&D, widespread adoption of new-age technologies such as AI/ML has not yet started. Information management tools, collaborative tools, automation, data aggregation and analytics, AI for ligand identification are some of the current top use cases.

Illustrative examples of pharma prioritising digitalisation in R&D

A leading pharma company

creates collaborative platform to improve R&D efficiency

A global pharma company

creates a digital lab to improve collaboration and innovation

A leading pharma company

uses data lake in R&D for analytics and to drive efficiencies

Top technology use cases currently in R&D

Information management tools, collaborative tools, automation, data lake and analytics, AI in pre-clinical research for ligand identification

However, in the upcoming years, R&D will garner significant focus, as the government and the ecosystem gears up to position India as a pharma innovator. The success of home-grown COVID-19 vaccine in India has set the right precedent, and regulations are likely to move in the direction that support innovation from India.

The Department of Pharmaceuticals also released a draft policy in Oct 2021, which is expected to improve R&D and innovation. It prescribes simplification of regulatory processes, usage of digital technologies to automate dossier review and workflows, and promotion of industry-academia collaboration. It also proposes to offer fiscal incentives and to incentivise private sector investment in research through various means.

As more support comes from the government for organisations to foray into research and innovation, digital transformation will be increasingly leveraged (for end-to-end digitalisation of processes, collaboration with research partners, and use of AI/ML in drug discovery and development) to enable robust R&D and clinical development.

Cloud adoption – A 20 percent increase in workloads in the past two years

- Like any other industry, the pharma sector in India is looking at cloud to transform their processes and businesses. A slow mover, due to tight regulatory controls, the pandemic has also prompted the sector to embrace cloud for process enablement, and improvement in turnaround and efficiency.
- It is noteworthy that people, processes, and technology implementation within pharma requires GxP compliance, which relates to good practices (Good Manufacturing Practices [GMP], Good Laboratory Practices [GLP] etc.). The objective is to have safe and quality products for consumption, and that data integrity is maintained for obvious safety reasons. According to FDA regulations, computer and related systems fall under the ambit of data integrity and compliance. This requires cloud to be GxP compliant across functions involved in drug development and manufacturing. GxP is enacted under FDA's 21 CFR (Code of Federal Regulations), wherein"part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations." Similarly, for European Union (EU), EudraLex Volume 4, Annex 11[1] is considered for computerised systems.
- Leading cloud providers are now offering case examples and detailed context to establish GxP compatibility of their cloud services. Other regulations, such as GDPR compliance are also key requirements within the industry, which are being increasingly addressed by the cloud providers. This, along with the impetus from the pandemic, is encouraging pharma companies to consider shifting their workloads on to cloud.
- On an average, leading pharma organisations witnessed a 20 percent increase in cloud workloads in the past two years.

One of the leading pharma companies in India highlights a **30 percent** reduction of development timelines due to the adoption of cloud services.

- However, organisations need a cloud strategy or roadmap for migrating their assets, and post implementation, a strong focus on governance, visibility, and monitoring.
- There is also limited understanding of shared responsibility, which is important for ensuring cybersecurity, data integrity, and privacy. As usage of AI and IoT engines on cloud increase, there should be a strong focus on data validation and protection.
- Pharma IT and security leaders continue to highlight the importance of incorporating cybersecurity in the cloud architecture.

Key cloud adoption challenges

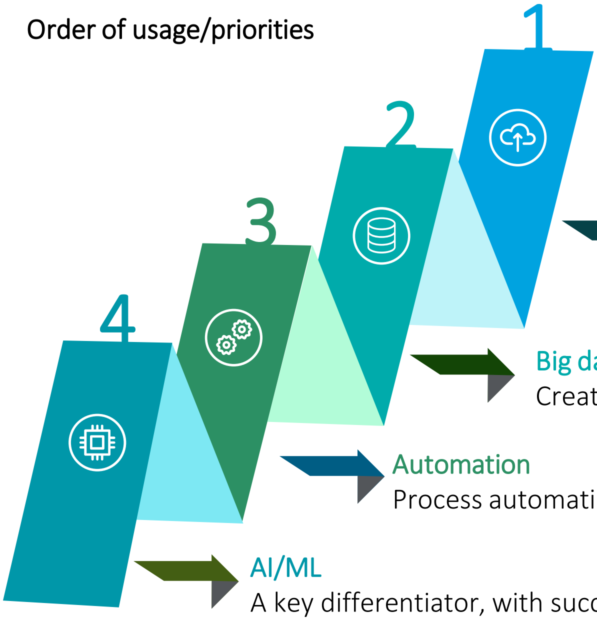
1. Lack of adequate know-how
2. Lack of a cloud strategy; more ad-hoc implementation
3. Lack of understanding of shared responsibility
4. Challenges with regulatory compliance
5. People, processes, technology not aligned for cloud implementation
6. Lack of visibility and monitoring
7. Fear of security breaches

Source: 1. EudraLex Volume 4, Annex 11

Use of digital technologies – Rising focus on AI/ML

Experts and respondents underline the omnipresence of cloud, big data/analytics, and automation, which are currently the most adopted technologies in the pharma sector. AI/ML and IoT are the next big arena. The industry has started to recognise AI/ML as a key differentiator, with the success of other technologies largely depending on embedding AI/ML solutions.

Order of usage/priorities



Cloud

Big data/analytics
Creating data lakes to derive insights across functions

Automation
Process automation with cognitive capabilities to enhance productivity

AI/ML
A key differentiator, with success of other technologies hinging upon its implementation

Source: DSCI-Deloitte analysis

Current use-cases of AI in leading Indian pharma companies include streamlining documentation, establishing Standard Operating Procedures (SOPs), managing incidents, implementing lean programmes, optimising supply chain, usage in drug discovery (in pre-clinical research for ligand identification), in creating digital therapeutics, etc.

Potential of AI across the value chain (not limited to)

Research and clinical development

- Target identification/validation
- Identifying novel pathways, disease Mechanism of Action (MoA)
- Molecular design
- Patient stratification
- Drug repurposing
- Trial design
- Pharmacovigilance

Manufacturing

- Quality control
- Automated batch release
- Optimising yield and output
- Streamlining documentation

Supply chain

- Better analysis and insights
- Forecasting, demand, and supply mapping

Launch and commercialisation

- AI omnichannel engagement
- Optimising customer interactions
- Creating digital therapeutics and personalised care solutions

Overall, AI and ML have the potential to solve many of pharma's R&D, manufacturing, and supply chain issues. At the same time, its applicability in the space of digital therapeutics can help in creating personalised treatments, thus, improving the quality of care. According to a Deloitte study[1], more than 40 percent of life sciences companies globally spent US$20-50 million in AI projects in 2019, and this was likely to increase going forward. Leading Indian pharma companies are also expected to follow suit.

Source: 1. Deloitte article - Scaling up AI across the life sciences value chain

India perspective

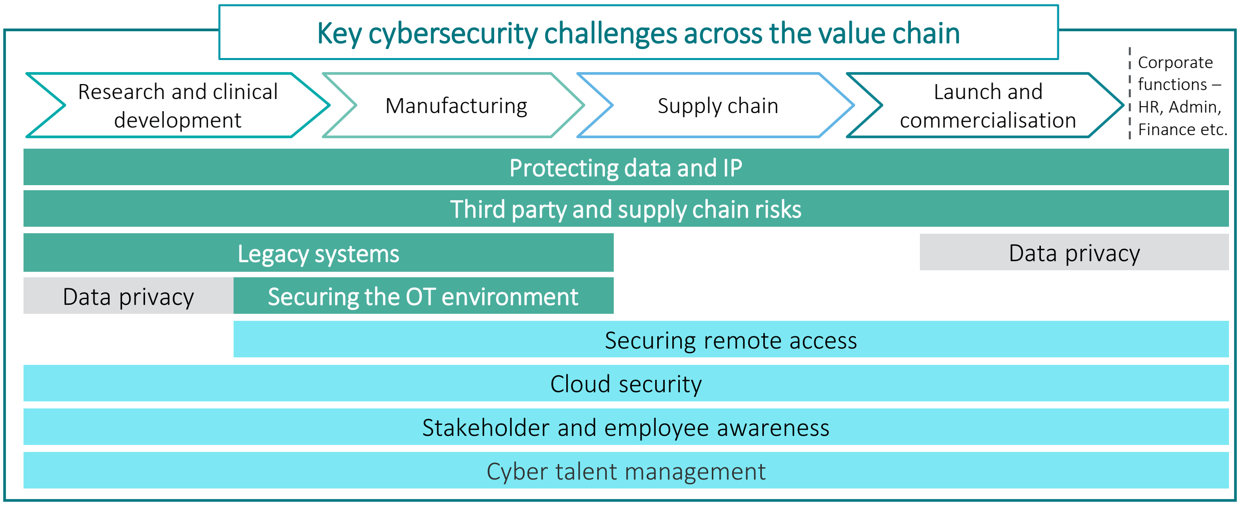
Cybersecurity

Impact of digital transformation and pandemic – Reimagining security strategies, measures, and controls

When the pandemic set in, remote accessibility became a challenge. Some leading firms had already embarked on the journey of digital transformation and remote operations, but enterprise-wide remote working and collaborations at-scale wasn't mature enough. The manufacturing systems were not prepared for remote operations, audits, or even repair, which also made the sector take cognisance that smart sensors and hyperconvergence across the factory floor was inevitable, going forward. Further to this, supply-chain optimisation, data-driven insights generation, and innovative means of outreach have always been important for the pharma sector. Such technology and digitisation bring in cybersecurity and privacy challenges, prompting CISOs and CIOs to rethink cybersecurity strategy, measures, and controls in their organisations.

Changes during the pandemic that enhanced security requirements

- Remote operations and remote collaborations at-scale, with emerging new use-cases
- Rise in the number and types of end-points connecting remotely
- Opening-up of the OT environment
- Increased use of third-party software and cloud solutions



Key cybersecurity challenges across the value chain

Research and clinical development

Manufacturing

Supply chain

Launch and commercialisation

Corporate functions – HR, Admin, Finance etc.

Protecting data and IP

Third party and supply chain risks

Legacy systems

Data privacy

Data privacy

Securing the OT environment

Securing remote access

Cloud security

Stakeholder and employee awareness

Cyber talent management

Source: DSCI-Deloitte analysis

🟩 Highest concerns 🟦 Moderate concerns ⬜ Lower concerns (mostly from other geographies)

Key trends

1. Globally, digital transformation and hybrid IT are perceived to be the top challenges, especially for pharma companies that are transitioning to become digital enterprises. Unsanctioned IT initiatives across the value chain is a pain-point, particularly in the US.
2. Across India, APAC, and the US, OT environment is increasingly becoming an area of concern for the CISOs, with the need for establishing proper strategy, governance, and monitoring.
3. In India, legacy systems, third-party risks, data and IP risks, and securing the OT environment are the top challenges that pharma security leaders face.
4. Data privacy requirements, currently come from other geographies as even emerging markets gear up for privacy requirements. It is noteworthy that pharma companies in India do not have direct patient data access, and a lot of privacy considerations are currently around employee and third-party data.

In India, the security challenges are pointed as pharma companies are currently embarking on their digital transformation journey. In the upcoming years, however, Shadow IT across functions is likely to become a problem. While experts opine decentralised model of security to manage shadow IT by stationing business security officers in various functions, each organisation needs to adopt a best-fit approach to maximise outcome.

Threats and vulnerabilities

According to Deloitte Global Cyber Threat Intelligence, in 2020, the threat actors capitalised on the COVID-19 crisis, using social engineering techniques to cash in on public fears. From launching malware-planting track and trace apps to phishing campaigns impersonating credible and government organisations, the threat actors added to the already existing woes. Across sectors, ransomware attacks were rising, also with double extortion techniques, where victim's data was exfiltrated prior to encryption, increasing the pressure of ransom payments. There were also several instances of state-sponsored attacks targeting nation-states, health organisations, pharmaceutical companies, and research institutes. India was not immune to such attacks given that the country rose to prominence with the home-grown COVID-19 vaccine. Around May 2021, fake apps that looked like vaccine registration apps were reported. Instead, they planted malware that could access personal details.[1] Security of OT systems is increasingly becoming a top concern for pharma companies as the leading organisations look to embrace newer technologies in production and supply.

For the pharma sector, ransomware attacks, IP and data theft continue to be the top causes of worry, both in India and globally. Stealing intellectual property, stalling production, and demanding ransom are some of the top motives, exacerbated by the pandemic. Pharma companies almost unanimously highlight phishing as the most common attack method.

Top vulnerabilities highlighted include security misconfiguration, unpatched systems, cloud vulnerabilities, distributed network, hidden backdoors, lack of access controls, new technology implementation, IT-OT convergence, sensors, and IoT devices.

But beyond specific targeting, the sector must also become aware of the threats and risks that come from various third-party associations. For example, the ransomware attack on a workforce management company in December 2021, created significant problems for its customers in processing payrolls. This also affected a global pharma company, where hourly staffers were either over-paid or under-paid. Any vulnerability in third-party organisations is likely to have an impact, which makes Third Party Risk Management (TPRM) a critical consideration for pharma companies.

Ransomware attacks, IP, and data theft were the top causes of worry for the sector, both in India and globally.

Phishing is the common attack method

- In October 2020, a leading Indian pharma company was attacked by ransomware. The lab immediately launched containment and incident management plan to limit the disruption
- In November 2020, another leading pharma company was attacked, which affected some of the systems.

Source: Media articles

Source: 1. India Today

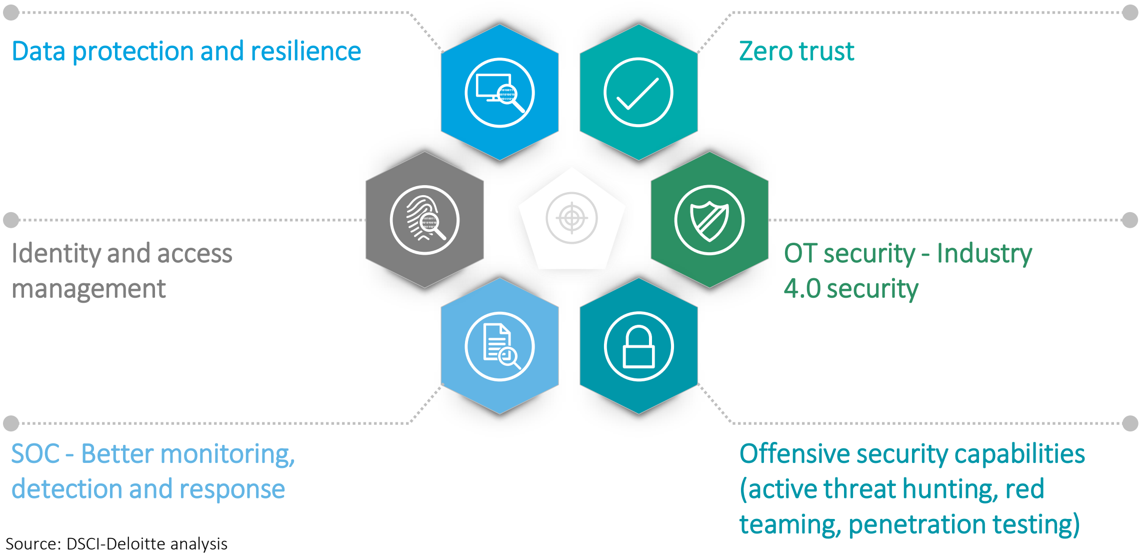
Security investments and priorities – A minimum increase of 25-30 percent in leading pharma companies

For leading pharma companies, cybersecurity investments have increased by a minimum of **25-30 percent** between 2019 and 2021, while for some, it has **doubled** in the past 18 months. The pandemic and the rising number of targeted attacks have prompted these security investments.

Areas of spending in the past 24 months: Security assessments, vulnerability assessment and penetration testing (VAPT), AI-based tools, active threat hunting, next-gen endpoint detection and response (EDR) and extended detection and response (XDR) solutions, network security, data security, identity solutions, UEBA, next-gen SOC, managed threat intelligence, education, and awareness.

Cybersecurity as a percentage of IT spending in leading pharma companies 5-8 percent

Six focus areas for leading pharma companies


Data protection and resilience
Zero trust
Identity and access management
OT security - Industry 4.0 security
SOC - Better monitoring, detection and response
Offensive security capabilities (active threat hunting, red teaming, penetration testing)

Source: DSCI-Deloitte analysis

- Leading organisations are increasingly prioritising data security and resilience as ransomware attacks, theft of IP, and nation-state attacks take centerstage. Organisations are considering multi-level data resilience, adopting cloud for data recovery and resilience.
- **Seventy percent of the leading pharma companies highlight focus on zero trust with the need for a clear roadmap in the next two years, around network, data, and access.**
- OT security and the need for creating secured factories is one of the key focus areas, as the sector takes the leap of Industry 4.0.
- Focus is increasing on security monitoring, covering all end-points, OT environment, and supply chain. Nearly 55 percent of the respondents highlight having a hybrid SOC (partly in-house and party outsourced), with more operations likely to be outsourced in the next couple of years. Managed detect and response, more coverage of end-points, SOAR, UEBA, breach and attack simulation are key areas of interest.
- Leading pharma firms are also looking for real-time threat intel, threat hunting, and dark web monitoring.

For organisations who have made significant investments in the past two years, their future investments are likely to stabilise, mostly focused on better third-party management, enhanced monitoring, optimisation through automation and outsourcing, and security with regards to digital transformation and new tech adoption. While those who haven't invested enough, are likely to invest in areas that leading pharma companies prioritised in the past 24 months.

Security governance in large pharma companies

Around 2017/2018, as digitisation started becoming more ubiquitous, cybersecurity started gaining prominence. Security as a function started off-shooting from the traditional IT, but it was the pandemic that transformed the way pharma companies would look at cybersecurity.

Cybersecurity governance

In leading pharma companies, security is predominantly managed by a CISO or a designation equivalent. While it may not be the case in other organisations, especially MSMEs, where the IT team oversees cybersecurity. Many companies started hiring a CISO from 2018/2019. The CISO budget is typically part of the IT budget, and the function is mapped to the CIO function.

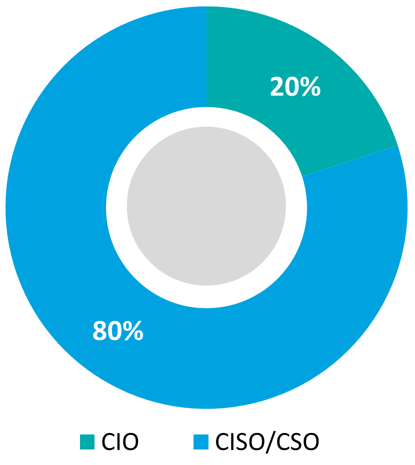
Privacy governance

Although in most organisations, privacy is under the ambit of a CISO, the governance structure is still evolving. There is a need for privacy mapping to the legal function, with technological mapping to the CISO or CIO function.

OT governance

OT typically falls under the engineering/manufacturing department; however, OT security governance is still evolving with the priorities and the dynamics of the organisation. Our research highlights the need for better collaboration to prioritise OT security. It is important to establish a joint governance comprising the senior leadership of IT, security, engineering, and management to provide the appropriate attention and security to OT systems. The need for specialised OT cybersecurity teams, mapped to the CISO function, is also emerging. This will encourage better measures, controls, and monitoring.

80% of large pharma organisations in India say that a CISO manages security in their organisation

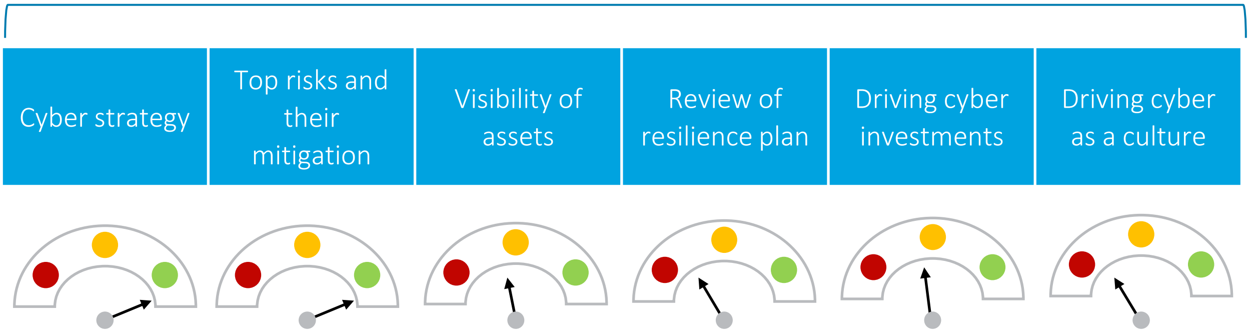


Source: DSCI-Deloitte analysis

Board and senior leadership alignment

Post the pandemic, cybersecurity has garnered a lot of attention. Security leaders and industry experts ‘strongly agree’ that board’s commitment towards cybersecurity has increased. Security leaders also highlight an increase in face time and cybersecurity representation and discussions at the board level. However, with regards to investments, there is a mixed reaction, particularly when it comes to showing RoI on security investments.

Board’s involvement and commitment to cybersecurity



Cyber strategy

Top risks and their mitigation

Visibility of assets

Review of resilience plan

Driving cyber investments

Driving cyber as a culture

What is expected from the **Board?**

- To drive cybersecurity as a culture, with a top-down approach
- To drive investments, by looking at the effectiveness of the cyber programme, from a strategic, operational, and business standpoint
- To link cyber resilience to business resilience, moving from RoI to resilience indicators, reviewing resilience plans, and taking part in simulation drills and cyber war gaming
- To acknowledge cybersecurity as a competitive advantage and a key indicator of responsible corporate governance

What is expected from the **security leaders?**

- To conduct table-top exercise, cyber war gaming for the board
- To have a clinical and methodical way of presenting, with examples, peer insights, and business correlation
- To identify the best-fit risk remediation strategy (whether to reduce the risk through investments or transfer the risk) using cyber-risk quantification and statistical models
- To bring in external partner and subject matter experts for audit and assurance

Source: DSCI-Deloitte analysis

OT security – Rising challenges due to IT-OT integration

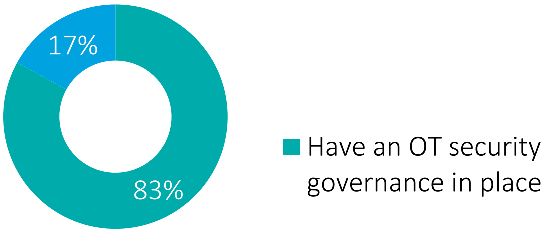
- Traditionally, OT systems have remained isolated, but with the rise in smart factories (with cloud, IoT and AI adoption), integrated supply chain management, and the need for remote operation management, the IT and OT environments are getting integrated.
- The OT environment within pharma and bio-pharma companies is extremely critical. A cyber attack causing malfunction, delay in production, tampering of information, and even theft of IP, can have huge repercussions not only on the organisation but also on people's lives.

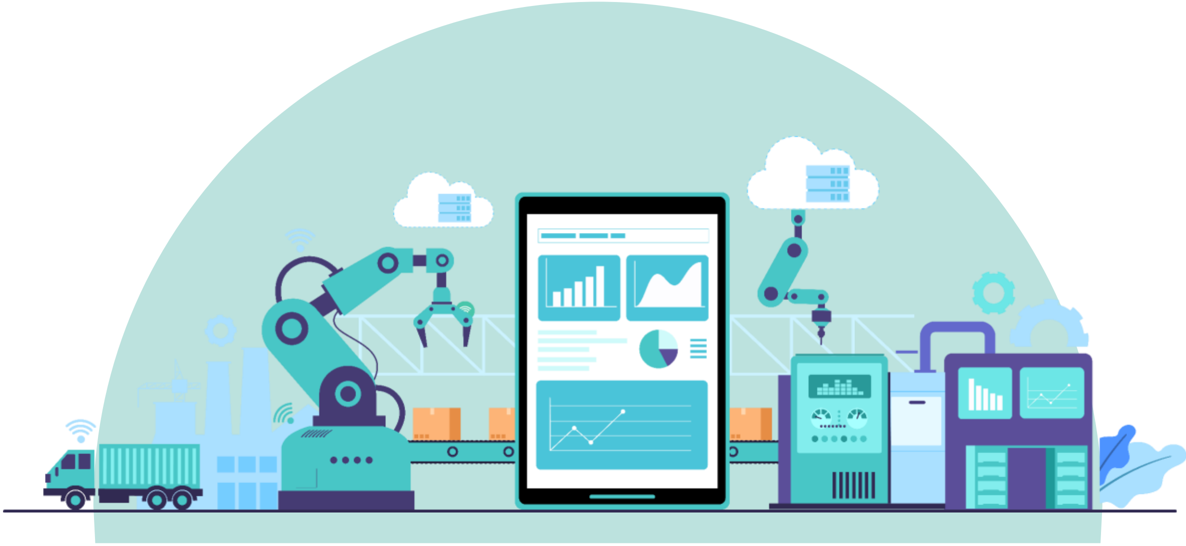
What is causing IT-OT convergence in the pharma sector?

- Rise in remote audits, enablement, and execution of processes; need for readying the systems for virtual FDA audits; need for providing remote access to original equipment manufacturer (OEM) providers
- Emergence of smart, connected factories - IIoT integration and use of cloud services

Securing the OT systems and network is becoming increasingly important as threat actors shift their focus to pharma companies. Organisations must be aware that opening the OT environment can make any threat in the enterprise network or third party to laterally move into the OT environment, in the absence of proper network segmentation and controls. OT systems are already vulnerable as many still use obsolete versions of operating systems and software. Certain challenges and gaps also exist with regards to system maintenance, security governance, employee awareness, and security monitoring, which needs to be addressed.

Leading firms indicate having an OT security governance; however, the need for joint OT-IT governance, with the involvement of leadership is important.





Key challenges for the OT environment as highlighted by leading pharma companies

1

Transitioning to Industry 4.0, and IT-OT convergence:
The pandemic catapulted the need for Industry 4.0/smart factories within the sector, for remote operability and streamlining of processes. Lack of a sound transition plan from complete physical air-gaps to Industry 4.0, without assessing interfaces, integration, and data exchanges, and without complete visibility across asset inventory, can be a bottleneck.

2

Legacy systems:
Globally, and in India, experts highlight the challenge of outdated/legacy systems, which may become a huge problem with IT-OT convergence. The complexity of the OT environment and the legacy systems make vulnerability management a challenging process. Patching and system upgrading requires assessments and reconsiderations on functionalities at an operational level. Any amount of downtime caused due to patching can impact operations.

3

OT security governance:
Seventeen percent of the leading firms highlighted lack of a well-defined OT security governance structure. OT being mapped to the manufacturing/industrial/engineering division, makes it occasionally difficult for security leaders to take cognizance of the OT security environment.

4

OT security monitoring:
The IT and security monitoring mostly happens at certain gateway level; however, there is a need for continuous monitoring of the OT environment through a converged IT-OT SOC, with specialised OT security professionals.

5

Security awareness:
As the manufacturing function gears up for Industry 4.0, lack of security awareness can pose a risk to the OT systems. OT engineers and employees could fall prey to social engineering attacks. Spear phishing and watering hole attack techniques can be used by threat actors to gain access to the OT systems. Similarly, infected drives and removable disks can also plant a malware even in an air-gapped environment.

Source: DSCI-Deloitte analysis

OT security – Success lies in enhanced cooperation

Best practices[1]

Enhanced IT-OT cooperation with joint governance for better management of security risks

Having a transition plan to Industry 4.0, from complete physical air gap to logical air gap to a full-blown integrated environment, all throughout keeping security in mind. But given the complexity of the OT environment, making security changes can be cumbersome. Hence, balancing ‘risk’ and ‘rewards of mitigation’ is important during the transition plan.

Refraining from using obsolete versions of web servers, operating systems, content management systems, libraries, or other software.

Establishing a robust OT security strategy in creating ‘factories of the future’, secured and resilient by design; following a defense-in-depth architecture for Industrial Control Systems, and IIoT security across devices, communication protocols, applications, and software.

Following standards such as IEC 62443 (Cyber Security for Industrial Control Systems) across policies, management, industrial IT, products, and components. Back in 2014, US FDA had integrated ISA’s ISA/IEC 62443 in its standard list[2].

Microsegmentation of the network, having Access Control Lists (ACLs) with periodic reviews, securing remote access, managing privilege access, conducting data back-ups, monitoring for visibility of networked assets and activity – some of the best practices to follow.

Establishing OT security governance must entail defining a CISO’s role and introducing OT security specialists/satellite OT security units mapped to the CISO function. There must be a governing committee comprising engineering, security, IT, and business leaders which can help in better collaboration and elevating OT security needs to a business level.

IT-OT SOC convergence for better monitoring, but with specialised OT security experts; important to have custom OT-specific playbooks and use cases

Having an incident response and crisis management plan in place, with frequent exercises and management reviews

Introducing employee awareness and training as a key aspect of OT security strategy

Source: 1. Deloitte paper - ‘Reimagining OT cybersecurity strategy’; 2. Automation.com

Supply chain security – Crucial, as threat actors probe the extended network for data and access

Case study

The 2017 NotPetya attack on Ukraine had a devastating impact on a global pharma giant. The organisation, in its Ukraine office, was running a software application, which got infected, with the malware spreading throughout the organisation. This became a pharma textbook case study of how a state-sponsored attack and a third-party software security flaw could cause losses in billions of dollars. The organisation recently won the insurance lawsuit, but amidst the rising geopolitical escalations and state-sponsored attacks, most insurance firms are re-looking at their policy wording, with an attempt to clearly define inclusions and exclusions around cyber terrorism, hostile situations, war-like actions, etc.

- Any vulnerability including malware attacks, piracy, unauthorised ERP access or unintentional/maliciously injected backdoors in purchased, open source or proprietary software, can have huge ramifications on organisations.
- But supply chain security is not just about third-party software. It brings into perspective the cyber risk environment and security in the entire extended enterprise network, wherever there is data sharing or infrastructure sharing. Unprotected systems in the supply chain have the potential to impact pharma processes. Particularly post the pandemic, threat actors are trying to exploit the extended enterprise network to gain access to credentials, IP, and research information. This makes overall TPRM a bigger imperative.

The importance of third-party risk management for the Life Sciences and Healthcare (LSHC) sector, according to Deloitte Global TPRM Survey 2021[1]

Key findings

- Fifty percent of the LSHC organisations experienced a third-party incident
- Amongst all risk domains within third-party risk management, cyber risks ranked second highest; with highest response from LSHC as compared with other sectors
- LSHC was more likely to want to improve their TPRM across real-time information, risk metrics and reporting, TPRM business processes, and people and organisational issues than other industries.

Source: 1. Deloitte Global Third-Party Risk Management Survey 2021

Supply chain security – Need for risk intelligence for better metrics and reporting

The India context

- Our research suggests that leading organisations have a TRPM process in place, but for most of the organisations, it is mostly policies and compliance checks, in the beginning of agreements, with lesser focus on tools and technologies, and real-time reporting.
- In the upcoming years, as supply chain security continues to baffle the pharma sector, more focus will be on risk intelligence and getting an end-to-end cyber risk view.
- Also, organisations are looking beyond just third parties, to include extended partner network (4th party, 5th party, etc.) to better manage risks using water-tight contracts, with liabilities and indemnities. As more organisations gear up to bolster the pharma value chain, leveraging the PLI schemes or otherwise, it is extremely critical that security becomes a key tenet in any third-party collaboration.
- Some of the leading organisations with global operations also highlight ISO 28001:2007[1] for supply chain management – implementing security, assessment, and plans.

Key outsourcing partners that pharma companies engage with include the following:

Contract research organisations, contract manufacturing organisations, IT solution providers, data management and analytics partner, supply chain partners, digital platform providers, startups, cloud providers, etc.

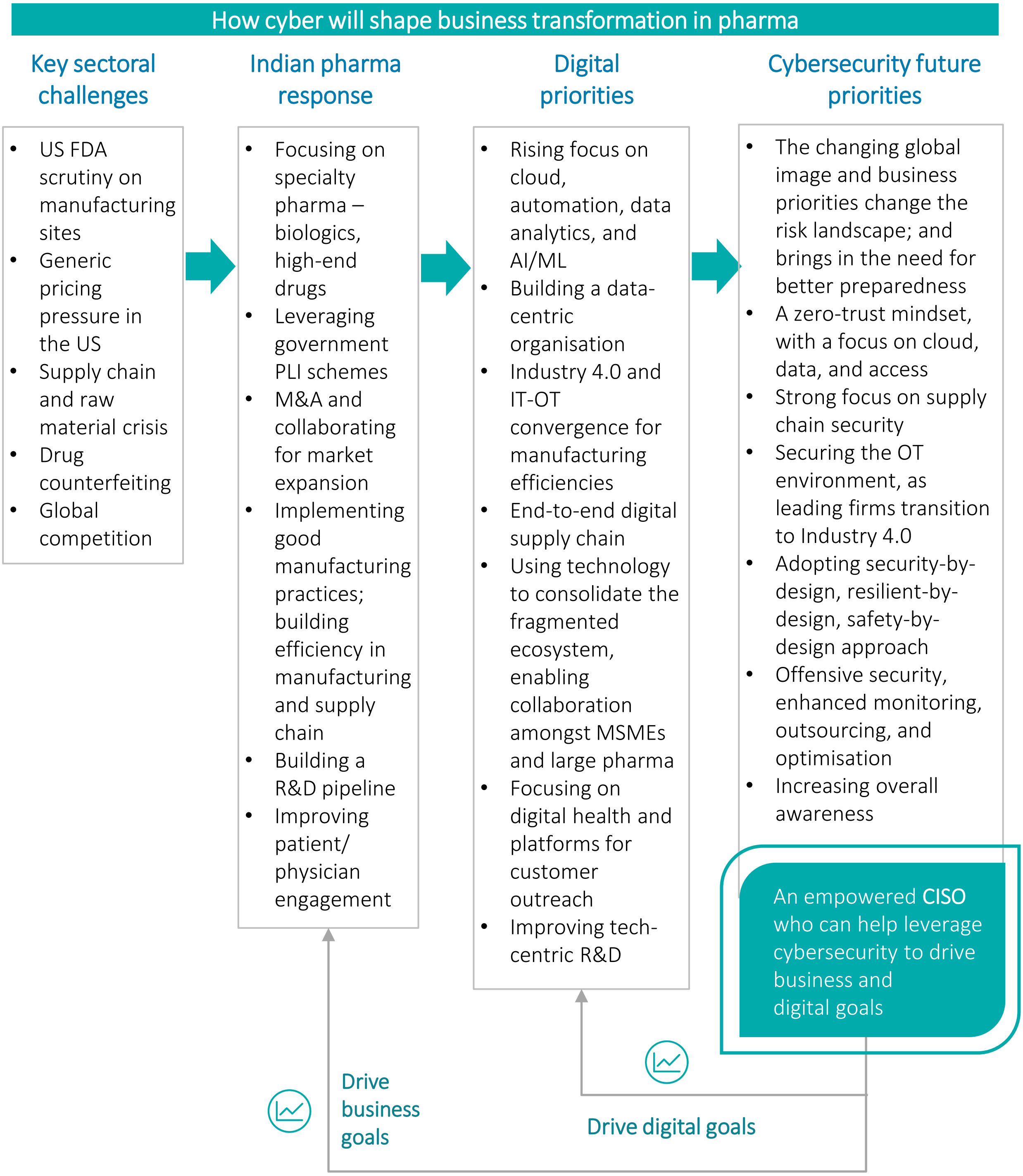
1. Detailed contractual requirements and disclosures on security and privacy, with partner mandates on end-point management, Identity and Access Management (IAM), data policy, etc.
2. More focus on risk intelligence (e.g., identifying risks through predictive analytics, risk stratification of suppliers, improving real-time information, risk metrics, and reporting
3. Licensed third-party auditors to certify certain potential partners
4. Zero-trust cloud for better collaboration and safe data exchange
5. Regular audits of open source and vendor source code – restricting third-party programmes' access and permissions
6. Education and awareness within the organisation and across the supply chain

Source: 1. ISO Webpage

Outlook and next steps

Cybersecurity as a key lever for business transformation and enablement

As leading pharma organisations gear up for the next stage of growth, there will be a continued focus on supply chain and manufacturing optimisation. Organisations are likely to explore innovative models of outreach and look at expanding their partner ecosystem. The surge in M&A is also likely, to build robust portfolios and expand the reach. It is imperative that **cybersecurity** remains a key consideration, to not just manage any cyber risk that comes along the way but also to truly enable business transformation in these organisations.



How cyber will shape business transformation in pharma

Key sectoral challenges

- US FDA scrutiny on manufacturing sites
- Generic pricing pressure in the US
- Supply chain and raw material crisis
- Drug counterfeiting
- Global competition

Indian pharma response

- Focusing on specialty pharma – biologics, high-end drugs
- Leveraging government PLI schemes
- M&A and collaborating for market expansion
- Implementing good manufacturing practices; building efficiency in manufacturing and supply chain
- Building a R&D pipeline
- Improving patient/ physician engagement

Digital priorities

- Rising focus on cloud, automation, data analytics, and AI/ML
- Building a data-centric organisation
- Industry 4.0 and IT-OT convergence for manufacturing efficiencies
- End-to-end digital supply chain
- Using technology to consolidate the fragmented ecosystem, enabling collaboration amongst MSMEs and large pharma
- Focusing on digital health and platforms for customer outreach
- Improving tech-centric R&D

Cybersecurity future priorities

- The changing global image and business priorities change the risk landscape; and brings in the need for better preparedness
- A zero-trust mindset, with a focus on cloud, data, and access
- Strong focus on supply chain security
- Securing the OT environment, as leading firms transition to Industry 4.0
- Adopting security-by-design, resilient-by-design, safety-by-design approach
- Offensive security, enhanced monitoring, outsourcing, and optimisation
- Increasing overall awareness

An empowered **CISO** who can help leverage cybersecurity to drive business and digital goals

Eight key security considerations

01

The changing global image and business priorities change the risk landscape; need for better preparedness

As the sector takes a centre stage in the global pharma narrative, it comes in the radar of threat actors, including the nation-state actors. Whether it is theft of IP, stalling of manufacturing plant, or a ransomware attack, cyber attack on pharma could not only lead to business and reputation loss, and jeopardise the Indian pharma narrative, but most importantly, has the potential to impact the lives of people. The pharmaceutical sector needs better cyber preparedness, across stakeholders and across the value chain, for effective cyber risk identification, management, and mitigation. As leading pharma companies gear up for increased M&A activities, it is also advisable to consider cybersecurity in M&A due-diligence. At the same time, having a risk transfer plan in place is important. Almost unanimously, leading pharma firms highlight the importance of cyber insurance. Cyber insurance is important not only for leading organisations, but also for mid-size and smaller firms as cyber risk coverage can pave the way for enhancing security, as the premiums get attached to security posture.

02

A zero-trust mindset with a focus on cloud, data, and access

Pharma sector's continued and rising focus on building a data-led enterprise, is almost palpable now in India. As a result, data protection and data security must become almost core to cybersecurity management in pharma companies. Cloud transformation has the potential to catalyse data-centric transformation and at the same time enable zero trust. While leading pharma organisations plan for a zero-trust strategy and architecture in the next 24 months, it is also important for smaller organisations and those addressing specific part of the value chain to have a systematic approach to data protection, data resilience, and managing both internal and third-party access.

03

Strong focus on supply chain security

As the leading firms in India expand their network, offerings and capabilities via partnership, a strong focus on TPRM is required. While most indicate having a TPRM-process in place, smaller firms don't have the same. Even in large firms, strong visibility and monitoring of supply chain risks by using risk intelligence tools is not very common. As the pharma supply chain gets interconnected and digitised, having robust processes, controls and accountability across partner firms is essential to mitigate supply chain risks. Even with regards to third-party software, audits of open source and vendor source code is essential.

04

Securing the OT environment, as leading firms transition to Industry 4.0

As Indian pharma evaluates the concept of Industry 4.0, with the possibilities of more edge devices and edge computing, and inter-connected factory floors, it is important to keep security at the core. While the newer facilities can be designed keeping cybersecurity and resilience in mind, changing existing processes will have an immediate impact on OT security. This requires defense-in-depth strategy, microsegmentation of the network, round-the-clock monitoring via an OT-IT next-gen SOC, and a joint governance for better accountability and business correlation.

Eight key security considerations - Continued

05

Adopting security-by-design, resilient-by-design, and safety-by-design approach

Every leading pharma organisation in India puts a strong focus on cyber resilience and crisis management, and there is a business and social imperative to do so, as availability is critical in such a sector. There is a rising focus on better incident management, with organisations prioritising ransomware resilience. Cyber crisis simulation, red-teaming, blue-teaming and purple-teaming should be prioritised by these companies. It is also important to embed cybersecurity into IT and business initiatives. As of date, several leading firms have not completely adopted DevSecOps. Full integration and implementation of DevSecOps in Software Development Lifecycle (SDLCs), along with secure code reviews, can truly help digital transformation initiatives become a success, irrespective of the business function that is being transformed and irrespective of the technology in focus.

06

Offensive security, enhanced monitoring, outsourcing, and optimisation

CISO function is becoming hybrid. The need for collaboration with cybersecurity subject matter experts/service providers, to better manage the security environment and securely transition to latest technologies, is becoming evident. From managing the unknown to the mundane, the CISO function is likely to engage with service providers, to bring in newer capabilities around offensive security and get a 24*7 monitoring of their IT and OT environment. Monitoring across assets and edge devices, monitoring using behaviour analytics, better detect and respond with XDR solutions, purple-teaming for better preparedness are some of the features of next-generation cyber fusion centres. Even small- and mid-size organisations can explore the concept of virtual CISO in the absence of a robust security team within the organisation.

07

Increasing overall awareness

Lack of awareness and basic security hygiene can prove detrimental. As social engineering attacks continue to increase, and phishing attempts get sophisticated, cybersecurity awareness must become mainstream. It is a business imperative now to democratise cyber and privacy awareness, with sensitisation across levels and the value chain. Leading firms also have the onus to spread cyber awareness in the partner network, whether amongst specialised contract manufacturers or digital startups.

08

An empowered CISO who can help leverage cybersecurity to drive business and digital goals

While experts and security leaders highlight that security conversations have significantly risen in value and focus, the need for security mapping into the risk function, more face time with the board, and empowering the CISO to effectively manage cyber risks across functions is critical. This also brings in board’s involvement and oversight. Now is the time to conduct cyber trainings, war gaming, and table-top exercises for the board and involve them into activities, such as reviewing the resilience plans to driving cybersecurity as a culture in the organisation. The CISO must also strive to become a business communicator, which can help in addressing business needs better.

Key recommendations for government to fortify the ecosystem include the following:

1. Scale up attestation to pharma sector on lines of critical information infrastructure.
2. Nodal bodies, such as CERT to engage with pharma CISOs for intelligence and best practices sharing.

Conclusion

It is interesting to note that India started the manufacturing of 35 APIs[1], which used to be imported earlier. The governments' PLI schemes are focused on bolstering manufacturing of not only APIs/KSMs/drug intermediaries, but also biologics and patented drugs. This is expected to provide a significant fillip to the sector.

Further, a 200 percent increase in FDI inflows[2] in the pharma sector positions India as a preferred destination to develop affordable and quality drugs. The government also highlighted the phenomenal growth of 103 percent in exports since 2013-14[3].

The world is beginning to appreciate the potential of the Indian pharma sector. With the right regulatory support, collaboration, and ecosystem development, the pharma sector is poised to become 'the pharmacy of the world'. There is no better time than now to use the power of technology and digital transformation across the value chain to catapult this growth and enable Indian pharma to set new paradigms in the global arena. The leading pharma organisations have already embarked on this journey, and are exploring cloud, big data/analytics, automation, and AI, to create smart and efficient organisations, and at the same time leverage the power of technology to create immense value for physicians and patients.

To be able to scale this vision and growth sustainably and create trust globally, the pharma sector requires an important 'cog in the wheel' and that's 'cybersecurity', which can help make the transition from a leader to a 'trusted leader'.

This goes beyond leading pharma companies in India. As more niche players enter the market, leading to enhanced collaboration and creation of a hyperconnected ecosystem, the security posture of the whole network must be enhanced to effectively combat cyber threats.

Source: 1. Swarajya; 2. Mint; 3. Press Information Bureau – Government of India

Abbreviations

Abbreviations

Acronyms	Full form
ACL	Access Control List
AI	Artificial Intelligence
APAC	Asia Pacific
API	Active Pharmaceutical Ingredient
APT	Advanced Persistent Threat
BEC	Business Email Compromise
CAGR	Compound Annual Growth Rate
CERT	Computer Emergency Response Team
CERT-In	Indian Computer Emergency Response Team
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CRO	Chief Risk Officer
DevSecOps	Development, Security and Operations
DSCI	Data Security Council of India
EDR	Endpoint Detection and Response
EEA	European Economic Area
ELN	Electronic Laboratory Notebook
ERP	Enterprise Resource Planning
EU	European Union
FDA	Food and Drug Administration
FDI	Foreign Direct Investment
FY	Fiscal Year
GDPR	EU General Data Protection Regulation
GLP	Good Laboratory Practices
GMP	Good Manufacturing Practice
GxP	Good Practice
HR	Human Resources
IAM	Identity and Access Management
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Intellectual Property
IQ	Installation Qualification

Acronyms	Full form
ISA	International Society of Automation
ISO	International Organisation for Standardisation
IT	Information Technology
KSM	Key Starting Material
LGPD	General Data Protection Law
LIMS	Laboratory Information Management System
LSHC	Life Sciences and Health care
M&A	Mergers and Acquisitions
MDR	Managed Detect and Response
MES	Manufacturing Execution Systems
ML	Machine Learning
MoA	Mechanism of Action
MSME	Micro, Small & Medium Enterprises
NASSCOM	National Association of Software and Services Companies
OEM	Original Equipment Manufacturer
OQ	Operational Qualification
OT	Operational Technology
PIPL	Personal Information Protection Law
PLI	Production Linked Incentive
PQ	Performance Qualification
R&D	Research and Development
RoI	Return on Investment
RoIC	Return on Invested Capital
SaaS	Software as a Service
SDLC	Software Development Life Cycle
SEC	Security and Exchange Commission
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operation Center
SOP	Standard Operating Procedure
TPRM	Third Party Risk Management
UEBA	User and Entity Behaviour Analytics
VAPT	Vulnerability Assessment and Penetration Testing
XDR	Extended Detection and Response

Connect with us

Deloitte

Rohit Mahajan
President, Risk Advisory
Deloitte India
rmahajan@deloitte.com

Gaurav Shukla
Partner and Leader,
Cyber, Risk Advisory
shuklagaurav@deloitte.com

Deepa Seshadri
Partner, Risk Advisory
deseshadri@deloitte.com

Jaishil Shah
Partner, Risk Advisory
jashah@deloitte.com

DSCI

Rama Vedashree
CEO, DSCI
ceo@dsci.in

Dr Sriram Birudavolu
CEO, Cybersecurity Centre of
Excellence, DSCI
sriram.b@dsci.in

Contributors

Deloitte

Sowmya Vedarth

Jaishil Shah

Manishree Bhattacharya

Kiran Wagge

Piyush Bajpai

Dr Vikram Venkateswaran

DSCI

Anand Raman

Dr Sriram Birudavolu

About

Deloitte

Deloitte is one of the world’s largest and most diversified professional services organisations, providing assurance and advisory, tax, management consulting, and enterprise risk management services through more than 345,374 professionals in more than 150 countries. Our organisation includes a unique portfolio of competencies integrated in one industry-leading organisation. Deloitte Touche Tohmatsu India LLP (DTTI LLP) is a member firm in India that provides non-audit consulting services. Our experienced professionals deliver seamless, consistent services wherever our clients operate.

In India, Deloitte is spread across 12 cities with over 12,000 professionals, who are proficient at delivering the right combination of local insight and international expertise to our clientele drawn from across industry segments.

Deloitte is well-equipped to deliver solutions to the complex challenges faced by organisations across the public and private sectors. Our edge lies in our ability to draw upon a well-equipped global network and teaming this with customised services at a local office.

We have been consistently recognised as leaders by Gartner in the Data and Analytics space, as well for Public Cloud Infrastructure Managed and Professional Services and Oracle Clod Application Services.

https://www2.deloitte.com/in/en.html

DSCI

Data Security Council of India (DSCI) is a not-for-profit, industry body on data protection in India, setup by NASSCOM®, committed towards making the cyberspace safe, secure and trusted by establishing best practices, standards and initiatives in cyber security and privacy. DSCI works together with the Government and their agencies, law enforcement agencies, industry sectors including IT-BPM, BFSI, CII, Telecom, industry associations, data protection authorities and think tanks for public advocacy, thought leadership, capacity building and outreach initiatives.

https://www.dsci.in/

Notes

Notes

DSCI

PROMOTING DATA PROTECTION

A NASSCOM® Initiative

This report has been jointly developed by Data Security Council of India (DSCI) and Deloitte. The information contained herein has been obtained or derived from sources believed by DSCI and Deloitte to be reliable. However, DSCI & Deloitte disclaims all warranties as to the accuracy, completeness or adequacy of such information. We shall bear no liability for errors, omissions or inadequacies in the information contained herein, or for interpretations thereof. The material in this publication is copyrighted. You may not, distribute, modify, transmit, reuse or use the contents of the report for public or commercial purposes, including the text, images, presentations, etc. without prior consent from either DSCI and/or Deloitte.

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.