Cybersecurity in the Pharmaceutical Industry

The expansion of the Internet of Things (IoT) and Industrial Internet of Things (IIoT) device integration has greatly increased the attack surface.

As the pharmaceutical industry grows, the danger of cyber attacks increases, putting sensitive operational technology and patient data at risk. But while hackers are better equipped and resourced than ever, pharmaceutical companies have found it difficult to keep up with increasing security demands.

Pharmaceutical and biotech companies suffer **more breaches than those in any other industry**, with

53%

of them resulting from malicious activity[1]

The Seven Cybersecurity Challenges Facing Pharma Today

1 An Expanding Threat Landscape

The global pharmaceutical market is worth approximately **$934.8 billion** and is estimated to reach over **$1,170 billion** in **2021**, with locations spanning all continents.[2]

The expansion of IoT and other digital innovations are contributing to the growing number of attack targets, including cloud migrations, connected medicine, and telehealth.

2 Network Complexity Is Increasing

The average cost of a data breach in 2020 was **$3.86 million**[3]

As pharmaceutical organizations add safety products to meet security or compliance requirements, they are faced with maintaining increasingly complex security systems.

This multi-product approach introduces numerous high-level problems:

- IT teams must be trained on multiple management and reporting systems
- Lack of communication between products means responses cannot be automated, fast, or effective
- Security teams need integrated solutions woven into the network infrastructure
- It is prohibitively resource-intensive to demonstrate compliance
- Separately managing security controls is time-consuming and wastes IT resources

3 Bridging the Cyber Skills Gap

The global shortage of cybersecurity professionals is now over **4 million** and must grow at **145% annually** to meet demand.[4]

While pharmaceutical companies can be strategic about attracting and retaining top cybersecurity talent, people with these skills will be scarce for the foreseeable future.

The average time to identify a breach in 2020 was **203 days**[5]

4 Working Across Networks and Acquisitions

Growth-by-acquisition strategies create security challenges when pharmaceutical acquisitions do not possess adequate or easily integrated security infrastructures.

5 Protecting IP, Your Most Valuable and Vulnerable Resource

Intellectual property (IP) is one of the US's most valuable assets, worth a total of $6.6 trillion. With the race to find treatments and even more effective vaccines in full swing, drug development IP is more valuable than ever and a major target for theft.

89%

of pharmaceutical and healthcare companies have experienced some kind of data breach.[6]

6 Meeting Compliance Requirements

In 2018, businesses spent **$1.3 million** on average to meet compliance requirements and were expected to put in an additional **$1.8 million**.[7]

As regulatory requirements become more complex, manually achieving network-wide visibility gets more difficult while demonstrating compliance becomes costly and time-consuming.

7 Convergence of IT and Legacy OT Environments

Legacy software and hardware are typical in pharmaceutical manufacturing and most operational technology (OT) systems were not created with security in mind. As OT and IT networks converge, they are suddenly exposed to an all-new threat landscape that allows cybercriminals to exploit inherited vulnerabilities.

Security breaches have increased
11% since 2018 and
67% since 2014.[8]

Stronger Cybersecurity Starts with Smarter Architecture

There are numerous hurdles to achieving security, from compliance pressures and network complexity to increasingly sophisticated attacks. Instead of solving each issue separately, Pharmaceutical companies should take a more efficient, comprehensive architectural approach. Fortinet provides the **automation**, **visibility**, and **fast threat response** to let you easily demonstrate compliance, become more efficient, and beat attackers at their own game.

Find Out More

[1] https://www.forbes.com/sites/forbesbusinesscouncil/2021/03/18/how-the-pharmaceutical-industry-can-secure-networks-to-avoid-cyberattacks/?sh=2b16b33e1eb3
[2] https://blog.marketresearch.com/the-growing-pharmaceuticals-market-expert-forecasts-and-analysis
[3] https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
[4] https://www.isc2.org/Research/2019-Cybersecurity-Workforce-Study
[5] https://www.capita.com/sites/g/files/nginej291/files/2020-08/Ponemon-Global-Cost-of-Data-Breach-Study-2020.pdf
[6] https://www.smarttech247.com/news/cybersecurity-threats-faced-by-pharmaceutical-companies-in-2021
[7] https://iapp.org/media/pdf/resource_center/IAPP-EY-Gov_Report_2018-FINAL.pdf
[8] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study