FORTINET

WHITE PAPER

Top 7 Cybersecurity Threats and Challenges Today's Pharmaceutical Companies Must Address

Executive Summary

As pharmaceutical companies increasingly digitize data and store it online, they become more susceptible to pharmaceutical cyberattacks. While the industry is comprised of a number of sub-industries with different business models and technology needs, they all must control extremely sensitive and valuable information and ensure an effective security framework. Drug and device manufacturers and biotech companies retain proprietary data ranging from secret formulas for patented drugs, to patient and customer information, to scientific research and advancements.

The industry is being attacked by adversaries adept at exploiting vulnerabilities and carrying out disruptive cyber campaigns. Cyber threats are used by a variety of bad actors with a range of intended system consequences. These attackers are better resourced and more capable of accomplishing disruption than ever before. In addition to hackers seeking financial gain, pharma companies also have to worry about the full capabilities of nation-states or other pharmaceutical companies with state sponsorship.

Consequences of a successful breach are dire and may include contaminated drugs, stolen intellectual property (IP), needing to repeat clinical trials, damaged reputation, downtime, litigation, and lost revenue.

In this white paper, we will explore the top threats and challenges pharmaceutical companies must overcome when securing their networks, and what's driving them.

A pharmaceutical company's most valuable assets are typically secret formulas for proprietary drugs and other large amounts of strictly confidential data. This makes pharmaceutical companies attractive to criminals because this data is incredibly valuable and can easily be sold on the dark web or ransomed.[1]

Primary Threats and Challenges To Pharmaceutical Security

Cybersecurity strategies in the pharma industry were historically driven by compliance requirements, for example, Health Insurance Portability and Accountability Act (HIPAA) security standards, but in 2020, pharmaceutical leaders realize this approach is no longer adequate. After a number of recent high-profile pharmaceutical data breaches, these leaders recognize the need to urgently take action. There are a number of common challenges to overcome across the industry.

1. Network complexity

As the result of years of "bolting on" whatever disparate security point product was needed to meet a specific security or compliance requirement, a majority of pharma companies are faced with maintaining very complex security systems. There are a number of high-level problems with this beyond the security gaps inherent with this approach.

- Security events are not detected or understood because end-to-end visibility is lacking
- Threat response cannot be automated and is not fast or effective due to lack of communication between products
- Demonstrating compliance is prohibitively resource-intensive
- IT resources are wasted on the time-consuming task of separately managing all the security controls
- IT personnel must be trained on all the different management and reporting systems

2. Aging OT environments and IT/OT convergence

Aging OT infrastructure is a fact of life as legacy software and hardware are hardly uncommon in pharmaceutical manufacturing. In almost all instances, these operational technology (OT) devices and systems were not created with security in mind and were dependent on an air gap for separation.

Prior to the surge in digital transformation, OT and IT were separate, independent networks. OT systems were considered relatively safe from outside threats because they were not connected to the internet. As digital innovation and business intelligence gains compel

OT networks to converge with IT networks to reduce costs, increase productivity, or gain competitive advantage, OT networks are suddenly exposed to the entire threat landscape. These technology advances offer cyber criminals the opportunity to exploit inherited cybersecurity vulnerabilities.

In 2018, 74% of OT systems were breached—causing damages to productivity, revenue, brand trust, intellectual property, and physical safety.[2]

3. Expanding attack surface

The attack surface has greatly expanded thanks to Internet of Things (IoT) and Industrial Internet of Things (IIoT) device integration via OT/IT convergence. A number of other digital innovations are also contributing to the large number of attack targets available in pharma networks.

Cloud migrations. As with the rest of the world, cloud deployments and Software-as-a-Service (SaaS) are becoming standard and the pharmaceutical industry must adapt security practices to accommodate this new reality. The convenience and scalability offered by these solutions is attractive, but some companies lack a genuine understanding of present cloud security capabilities. Larger organizations also find their cloud migrations slowed by dependencies on legacy systems and security arrangements.

Connected medicine. Patient expectations are compelling care providers to put more systems online, which often translates to connecting internal systems. In addition to protecting data, this has relevant security implications for the drug and device manufacturers as they must safeguard intelligent devices that in some instances are capable of dispensing medicine. A combination of technological innovation and patient expectations set by other industries is making medicine a more connected industry than it was even a few years ago. Care providers and manufacturers are launching patient-facing apps that integrate with hospital systems. In some cases, they also access systems further upstream in the pharmaceutical supply chain.

This trend is placing new demands on security organizations at pharma companies that may not have experience involving endpoints and infrastructure that they don't fully control. With network resources being exposed to threats by potentially unsecure access, ensuring effective cybersecurity on the local-area network (LAN), wide-area network (WAN), and cloud edges—where data is generated and consumed—is challenging.

Endpoint proliferation. More and more devices, both company-owned and personal, are finding their way into corporate networks. The rapid growth and integration of mobile technology has transformed how pharmaceutical companies execute business. However, this proliferation of potentially vulnerable and possibly infected endpoints brings two types of security problems. One is, of course, that infected endpoints then infect the network. The second problem is that IT experts may not even know what is connected to the network.

Telework. When pharma companies around the globe suddenly shifted to telework due to the 2020 pandemic, myriad new attack vectors opened up to all types of security threats. Remote users create additional security requirements and different security challenges than on-site workers. For industries such as pharma, which have typically not had many employees working from home, implementing secure IT infrastructure for a remote workforce is a daunting but necessary task. Nearly two-thirds of respondents in a recent survey reported an increase in breach attempts and 34% experienced a breach during the shift to telework.[3] Further, a number of surveys have found that organizations plan to allow much more telework in the future than they had pre-pandemic, even after the health risk subsides.

4. Acquisitions and distributed networks

Many pharmaceutical companies are pursuing growth by acquisition, but this strategy creates security challenges since the acquisition targets rarely, if ever, possess adequate security infrastructure. The phenomenon is well known throughout the industry, but remains a persistent challenge. Such acquisitions need to consider cybersecurity best practices as part of connecting to an already complex web of affiliated and unaffiliated research sites, subdivisions, and distribution partners.

These pharmaceutical entities and branch offices routinely access and transfer intellectual property, electronic protected health information (ePHI), and other sensitive operational data. Owing to their disconnected systems, pharma enterprises struggle with challenges of visibility, data control, access auditing, and compliance reporting throughout their networks

5. Cybersecurity skills shortage

Security talent is difficult to find. The global shortage of cybersecurity professionals exceeds 4 million today, and the global cybersecurity workforce must grow at 145% annually to meet the demand for skilled cybersecurity talent.[4] Skills gaps occur most often in specific functional areas such as DevOps, the cloud, and IoT.[5] While pharma companies can be strategic about attracting and retaining top cybersecurity talent,[6] individuals with these skills will be scarce for the foreseeable future, making it difficult—and expensive—to fill new positions.

6. Insider threats

Insider threats pose significant risks to pharmaceutical companies. A recent study reveals that 30% of all breaches are caused by malicious or negligent insiders.[7] Damage from insider sources can be hard to detect because these threats encompass a wide range of behaviors and motives. It could be a disgruntled employee attempting to disrupt operations, a staff member looking to earn extra cash by selling customer data, or a well-intentioned co-worker who merely sidesteps a company policy to save time. Organizations often underestimate the potential impact of insider threats, but the good news is that they can be mitigated.

7. Compliance obligations

With the changing requirements and increased complexities of meeting regulatory compliance, the difficulty of manually achieving networkwide visibility and enforcing the required security controls only increases. Further, demonstrating compliance can be prohibitively time-consuming, especially when networks are comprised of disparate point products that don't share reporting capabilities.

Pharmaceutical companies have historically tailored security investments to meet compliance obligations. HIPAA, General Data Protection Regulation (GDPR), and GxP standards drive planning. But the reality is that most organizations struggle to demonstrate comprehensive compliance. For example, 56% of organizations say they cannot determine compliance for endpoint devices.[8]

In addition to avoiding fines or other consequences of not meeting compliance, there are many other considerations for pharma. "Data integrity has become a very important regulatory issue, alongside patient safety and product quality, especially as analog processes are increasingly being replaced with digital ones."[9]

When a company is acquired by another company, or the two companies merge, there can be a lot of shuffling, which means that cybersecurity strategies and approaches can change overnight. It also means that if a company's data is compromised, or they are found not to have taken enough care to safeguard their assets before a merger or acquisition is finalized, it could compromise the deal and leave the company vulnerable to legal problems.[10]

Conclusion

Pharmaceutical companies face a number of cybersecurity challenges ranging from network complexity to antiquated OT systems to compliance. The first step to solving all of these issues is to take a cohesive architectural approach to network security. This will provide the visibility, automation, and fast response to threats required to thwart attacks and easily demonstrate compliance.

[1] Andrew Douthwaite, "Cybersecurity – Why Pharmaceutical Companies Are Vulnerable to Cyberattacks & What You Can Do to Protect Your Company," Drug Development and Delivery, January/February 2020.

[2] "2020 State of Operational Technology and Cybersecurity Report," Fortinet, June 30, 2020.

[3] "Enterprises Must Adapt to Address Telework Security Challenges: 2020 Remote Workforce Cybersecurity Report," Fortinet, August 14, 2020.

[10] Andrew Douthwaite, "Cybersecurity – Why Pharmaceutical Companies Are Vulnerable to Cyberattacks & What You Can Do to Protect Your Company," Drug Development & Delivery, January/February 2020.

[4] "Strategies for Building and Growing Strong Cybersecurity Teams: (ISC)² Cybersecurity Workforce Study, 2019," (ISC)², 2019.

[5] "The Life and Times of Cyber Security Professionals: 2nd Annual Results Global Study: Cyber Security Skills Crisis Causing Rapidly Widening Business Problem," ISSA and ESG, November 9, 2017.

[6] "The Head of Network Engineering and Operations: A Highly Strategic and Integrated Technologist, Understanding the Cybersecurity Skills Shortage: An Analysis of Employer and Jobseeker Skills and Occupational Demographics," Fortinet, July 11, 2019; "The CISO Ascends from Technologist to Strategic Business Enabler, Understanding the Cybersecurity Skills Shortage: An Analysis of Employer and Jobseeker Skills and Occupational Demographics," Fortinet, September 5, 2019.

[7] "2018 Breach Data Investigations Report," Verizon, April 2018.

[8] "The Cost of Insecure Endpoints," Ponemon Institute, June 2017.

[9] Walter Pytlik, "Cybersecurity is an important issue for the pharmaceutical industry," Healthcare Industry BW, January 16, 2019.

FORTINET

www.fortinet.com

September 17, 2020 12:38 AM

779893-0-0-EN

D:\Fortinet\White Paper\Grey White Paper\GREY - Pharma\wp-FA-top-7-cybersecurity-threats-and-challenges-9172020