FORTINET

Top 5 Cybersecurity Threats and Challenges to Pharmaceutical Businesses for 2022

Executive Summary

Today's pharmaceutical companies are witnessing unprecedented change driven by a cocktail of competing factors – changing customer demands, increased global competition, pressures to innovate, hybrid working, supply chain disruption, regulation compliance and the need to reduce costs – which are all combining to create a challenging climate. While digital transformation, accelerated by the Covid-19 pandemic has helped to alleviate some short-term issues, certainly in terms of business continuity, it has also inadvertently opened the door to increased cyber risk.

Unfortunately, it is a fact of business life today that cyber criminals are increasingly attracted to data-rich companies that can provide a good return-on-investment for their activities, and pharmaceutical organizations increasingly fit the profile. The reality is that cyber threats evolve as criminals look to exploit new opportunities. As KPMG suggests[1], tactics are changing:

"Unlike auto-spreading ransomware such as WannaCry and NotPetya, many new strains open the door for criminals to steal data and manipulate systems, as attackers exhibit deeper knowledge and understanding of their target's environment."

Despite this increase in sophistication, the cyber criminal threat is still not ranked as a number one challenge by pharmaceutical businesses, according to Deloitte research[2]. As the need to protect IP and sensitive data is of paramount importance to the ongoing competitiveness of any pharmaceutical business, this needs to change.

The problem many pharmaceutical companies face is complexity. The rush to digitize to enable remote working, for example, has only added to the threat surface. Bolted-on technologies due to the pandemic have led to a mix of digital and legacy operational and infrastructure technologies that are difficult to secure. It leads to operational data silos and an attack surface that expands to remote working points and across ecosystems to suppliers and partners, who have their own hybrid working and rapid digitization challenges.

As organizations continue to pursue transformations, for greater customer-centricity and reduced costs, there is an increased shift to cloud-based infrastructures, tools and ecosystems. Partnerships with businesses of differing sizes brings additional complexity, methodology challenges and potential risk. Not all companies are consistent when it comes to mitigating cyber threats.

This myriad of connections and disparate devices need to be identified and protected as a whole, swathed in a secure, intelligent fabric that can mold to and meet the specific needs of each organization. A piecemeal approach to security will fail. The consequences of a successful breach are dire and impact every facet of a pharmaceutical organization, putting drugs, IP, clinical trials, reputation, and revenue at risk. It is therefore imperative that pharmaceutical organizations grow their understanding of the changing threat landscape, and with it, their understanding of how those threats can be stopped.

To that end, this white paper explores the top threats and challenges pharmaceutical companies must overcome when securing their networks, and evolving their businesses in this rapidly changing, technologically-driven industry. We look at the increasing sophistication of cyber threats, the vulnerability of aging, operational technology environments and the challenges of balancing the needs of growth with mitigating risk. After all, where there is risk, there can also be reward but it takes a holistic approach to cyber threats to make that happen.

"Unlike auto-spreading ransomware such as WannaCry and NotPetya, many new strains open the door for criminals to steal data and manipulate systems, as attackers exhibit deeper knowledge and understanding of their target's environment."

KPMG

Primary Threats and Challenges to Pharmaceutical Businesses

To protect IP and ensure data privacy, pharmaceutical organizations need to urgently address a number of common challenges. Below are the top five threats we've noticed across the industry:

1. Increasingly Sophisticated Cyber Threats Probe Complex Networks

As pharmaceutical spending is expected to grow by $367 billion during 2021[3] the market faces the prospect of increased attention from cyber criminals, attracted both by the value of data and IP but also perceived weaknesses in cyber defenses. Cyber criminals are growing increasingly sophisticated in how they use threats to target pharmaceutical companies. As Accenture's Cyber Threat Intelligence Report 2021[4] reveals, both targets and tactics are changing:

"Ransomware actors are expanding data leak extortion, devising new methods to pressure victims. Their creative approaches are hitting home as they place operational resilience—already tested by the disruptive forces of the pandemic—under increased pressure."

Internal Fortinet research[5] found that there was a tenfold increase in ransomware in the first six months of 2021 and that Q1 saw a botnet spike, with the percentage of organizations detecting botnet activity jumping from 35% to 51%.

It's clear that both the scale and sophistication of attacks pose a growing threat to vulnerable networks with multiple, distributed end points. This naturally impacts how pharmaceutical companies should address threats. The challenge is how to mitigate risk across multiple devices and complex networking structures that have rapidly evolved since the start of the pandemic. One way to mitigate these risks across multi connected devices is to enable a more secure VPN.

There is an urgent need for better VPN solutions and secure network access. Given that on average, it can take 257 days for pharmaceutical companies to identify a breach, the need for more sophisticated detection and reporting becomes essential. While pharmaceutical businesses have for a long time managed risk and compliance, the growing number of remote and off-site employees, and resulting cyber threat represents a new, unpredictable challenge that needs expert consideration. If end-to-end visibility is lacking, overall security, especially in the face of growing attacks on pharmaceutical businesses, suffers.

2. Security as a Priority: Changing Attitudes and Perceptions of Risk

Digital transformation and an increasing reliance on data is a universal trend. McKinsey reports[6] that Covid-19 has accelerated this change, as digital adoption delivered five years of growth in just eight weeks in the early part of 2020. The pharmaceutical sector is seeing similar change, and a Deloitte C-suite survey[7] of pharmaceutical companies point to R&D, global markets and the digital/IT transformation of functions, as the top three strategic business priorities for the next 5 years.

With this in mind, it is important to consider the impact a data breach would have on a pharmaceutical business. According to one study[8], pharmaceutical and biotech companies suffer more than most businesses. The study claims that 53 percent of organizations in these sectors have already suffered from malicious activity, with the average cost of a breach in a pharmaceutical business standing at over $5m. This is more than the healthcare, energy and financial services industries.

Data security needs to be a key feature of any business development, including expansion, restructure, mergers and acquisitions, or, as we have seen in recent months, a seismic shift in working practices. Cyber security, more than ever before, has to be a priority requirement for pharmaceutical businesses.

The average cost of a breach in a pharmaceutical business stands at over

$5m

3. Connecting Operational Technology and Avoiding Operational Outages

Pharmaceutical companies have been front and center in researching and developing vaccines against the Covid-19 virus. As Harvard Business Review suggests in a recent article[9], this would have been impossible without the enabling capabilities of a cloud computing platform. While this remains a phenomenal achievement, the reality is that too many pharmaceutical businesses retain legacy equipment within this structure, certainly within operational technology (OT) infrastructures.

Aging OT infrastructures are not uncommon in pharmaceuticals, especially in the larger, more established businesses. In some instances, legacy equipment can be over 20 years old and may no longer be supported with suitable security patches, or even worse, may never have had security at all. For the sake of operational continuity, avoiding outages and ensuring compliance, there needs to be a focus on a security fabric that can prevent IP and data theft, regardless of the age of systems.

When linking OT with cloud-based network IT infrastructures, the challenge becomes how to secure these newly connected systems. In some instances, large volumes of research data is accessed, analyzed and moved across these networks, risking years of work and valuable IP reputations, so the need to find a more intelligent, inclusive approach, that secures the link, is paramount, as is the need for the ability to monitor this newly expanded multi-cloud environment. Pharmaceuticals need adaptive cloud security to enable necessary visibility and control across cloud cyber security infrastructures for secure applications and connectivity from data center to cloud.

As pharmaceutical businesses look to converge these networks, to reduce costs as well as increase productivity, there is an increasing need to mitigate unforeseen risk in cyber criminals targeting what they would consider a weak point in pharmaceutical infrastructures.

4. Enabling Hybrid Working While Managing Compliance and Security Risk

The challenge most security advisors currently still face is the difficulty in network and device security due to the influx of remote working and employees operating off-site. The rapid increase in risk is, of course, understandable, as more remote devices connect to business networks and share data across potentially insecure Wi-Fi. Securing the network and business communications becomes an urgent priority, as employees access email and data via a proliferation of remote mobile devices, such as cell phones, tablets, and laptops.

Clearly, pharmaceutical companies see this as one of their biggest threats and hybrid/remote working is not going away anytime soon. As McKinsey suggests[10], most organizations are facing similar challenges over hybrid working. If anything, there is a disconnect between how and where employees and employers want work to be carried out. This raises the potential for disgruntled employees and an insider threat to data. It's therefore key that each organization has a clear and fair policy for the long term, and a security capability that can manage the diverse requirements of the future of work, including the movement of people and proliferation of remote devices.

There are also concerns around employee cybersecurity education and human error, leaking data, more by accident than design. Securing the data across OT and IT networks and out into remote technology environments will require security capabilities that can free up pharmaceutical businesses from complex security integrations. A single-platform approach with a security fabric that can reach across an entire organization regardless of size and location will solve the issue of vulnerable patchwork security. No more point solutions, acquisition-based vendor portfolios and best-of-breed integration-heavy solutions from GSIs.

On average, it can take

257

days for pharmaceutical companies to identify a breach.

5. Securing Complex Ecosystems: The Partner and Supplier Challenge

As PwC suggests in its supply chain report[11], "in order to meet the demands of a fast-evolving marketplace and the shift from patient to outcome, the pharmaceutical supply chain will need to undergo a radical overhaul."

> "In order to meet the demands of a fast-evolving marketplace and the shift from patient to outcome, the pharmaceutical supply chain will need to undergo a radical overhaul."
> **PwC**

The diverse demands of modern healthcare markets, coupled with increasing regulatory demands in sustainability and provenance, for example, are forcing pharmaceutical businesses to re-address supply chain partnerships and collaborations. With the growth of digital platforms and the ability to share data easily across those platforms, the risk of data theft multiplies.

The complexity of these pharmaceutical ecosystems is made even more intricate as a result of M&A activity, meaning security becomes increasingly complicated as new people and businesses bring a variety of different approaches and technologies to data security. It can lead to potential weak points, especially as the attack surface continually expands with new partners in new territories. As the saying goes, you are only as strong as your weakest link and with such complex ecosystems, there is potential for many weak links. For example, smaller R&D partners can represent an increasingly critical point of entry to malicious actors. If small partners do not have the budget or skills to secure data, they could be a weak access point for cyber criminals to reach data being shared throughout the ecosystem.

Conclusion

Security In Sync: End-to-end Protection that Grows with the Business

These are both exciting and challenging times for the pharmaceutical industry. On the one hand, you have a changing demand for products and services. The rise of personalized care and focus on outcomes, for example, is leading to the rapid adoption of digital technologies throughout the healthcare sector. Customer demands are changing, which is impacting how pharmaceutical companies are addressing functions such as communications, ordering, product delivery, and support. This in turn impacts R&D and manufacturing. There is also the added pressure of increased global competition and the ongoing need for compliance.

Every pharmaceutical company has had to adapt and in the past 18 months, adapt again and quickly. To be resilient and competitive, we have seen an increased adoption of digital technologies. While there is no doubting the need for these digital transformations, they come with a caveat – the more you connect the more you open a potential door for cyber criminals. This has only been exacerbated by the growth in remote working.

A number of high-profile pharmaceutical data breaches over the past couple of years have illustrated both the industry's attraction to cyber criminals but also its vulnerability. Pharmaceutical data and IP has a lot of value and cyber criminals understand that the industry is going through a transformation, where potential weak points in networks can be exposed.

The challenge for every pharmaceutical company is how to close that door quickly and efficiently. It demands a cohesive platform approach that will provide the visibility, automation and fast response required to stop attacks and be compliant - an integrated security platform capable of end-to-end protection and segmentation of everything from data and remote devices through to network infrastructures and ecosystems.

Learn more about how Fortinet can help protect your Pharmaceutical organization against dynamic and increasing cyber threats.

[1] home.kpmg/xx/en/home/insights/2021/04/ransomware-attacks-in-life-sciences
[2] deloitte.com/us/en/insights/industry/life-sciences/pharmaceutical-industry-trends
[3] iqvia.com/insights/global-medicine-spending-and-usage-trends-outlook-to-2025
[4] accenture.com/PDF-158/Accenture-2021-Cyber-Threat-Intelligence-Report
[5] fortinet.com//fortiguard-labs-threat-landscape-report-highlights-tenfold-increase-in-ransomware
[6] mckinsey.com/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days
[7] deloitte.com/insights/industry/life-sciences/pharmaceutical-industry-trends
[8] ibm.com/account/reg/uk-en/signup?formid=urx-46542
[9] hbr.org/2021/03/what-ceos-need-to-know-about-the-cloud-in-2021
[10] mckinsey.com/business-functions/organization/our-insights/its-time-for-leaders-to-get-real-about-hybrid
[11] pwc.com/gx/en/industries/pharmaceuticals-life-sciences/publications/pharma-2020/pharma-2020-supplying-the-future