
EVIDEN
Attacks on the system
Boosting security in pharmaceutical
and life sciences organizations
an atos business

Contents

With cyberattacks increasing in life sciences, we explore the impact of today's targeted attacks, highlight 2023's key investment areas and look at why security is a board level issue, not only an IT responsibility, that constitutes a business challenge.

1 Analyzing attacks on pharmaceutical systems

In our increasingly digital world, few senior leaders are unaware of the broader issues surrounding security and information governance, or the need to effectively secure systems and data to prevent breaches.

Certainly, over the past few years we have seen pharmaceutical companies and life sciences systems increasing targeted by 'bad actors'.

FTI Consulting (NYSE: FCN) recently announced a new survey and report, US Healthcare & Life Sciences Industry Outlook 2023. The report found more than two-thirds (70%) of US healthcare and life sciences companies experienced a cyber attack or incident during the last 12 months with malware/ransomware (31%) and phishing (27%) emerging as the most common incident types[1].

What makes the situation worse is that nearly half of all pharmaceutical companies have more than 1,000 leaked employee credentials exposed on the deep web. This situation opens the door to future phishing campaigns.

[1] https://www.fticonsulting.com/about/newsroom/press-releases/fti-consulting-survey-finds-more-thantwothirds-of-healthcare--life-sciences-companies-experienced-a

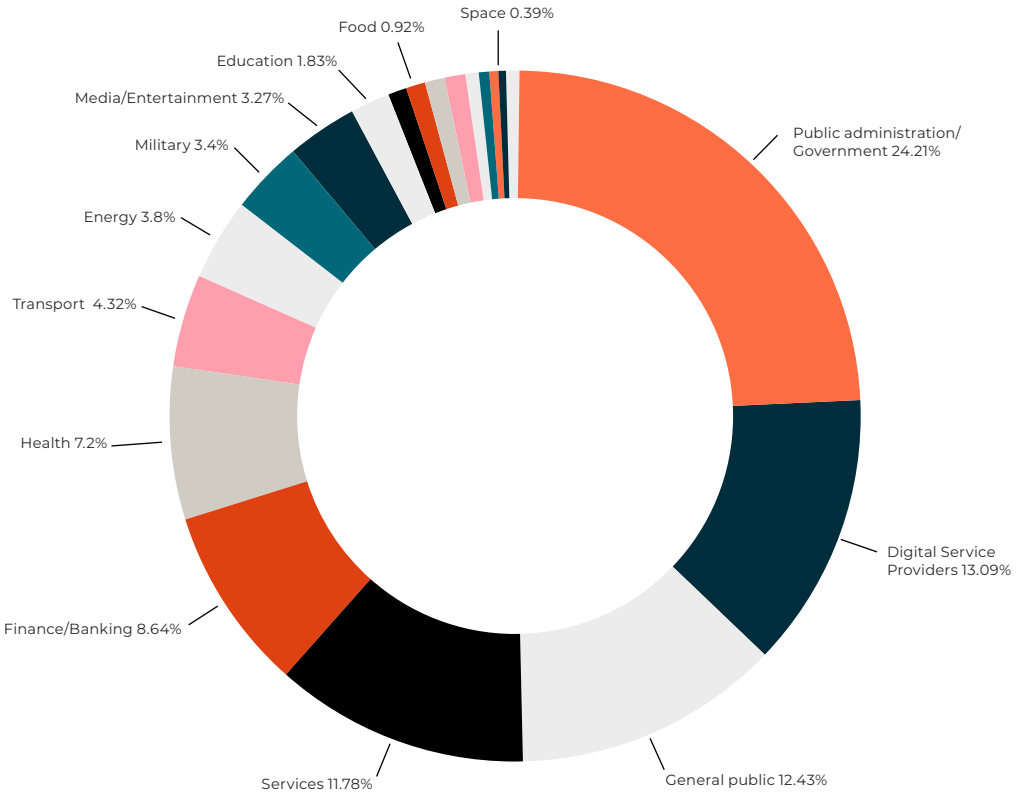
In 2020, vaccine makers were targeted by huge cyberattacks. Pfizer/BioNTech's documents on the vaccine were unlawfully accessed, stolen and illegally released online.

In the same period, AstraZeneca and 5 other drug developers were targeted by North Korean hackers through a phishing campaign. The objective was to gain access to employee's computers by sending out messages with malicious links or attachments. More globally, the COVID-19 cold chain was targeted by cyber adversaries.

Cyberattacks also target Internet of Medical Things (IoMT) that are widely leveraged by life sciences companies. In 2021, Medtronic, a leading medical device company in the US, had to recall insulin pump controllers due to potential hacking vulnerabilities. However, in September 2022, another vulnerability was found in one of their features, which could allow unauthorized access to insulin pump systems. This could potentially lead to dangerous outcomes, such as delivering too much or too little insulin to patients, resulting in severe harm or death.

Geopolitical events aside, there is no doubt that pharmaceuticals have been in the firing line for some time – from criminal hackers looking to extort money to well-funded state-sponsored hackers bent on creating maximum disruption. And as digital perimeters expand, the threat is heightened and the need for constant vigilance and tougher security measures continues to grow. Indeed, according to the European Union Agency for Cybersecurity, attacks against the healthcare sector surged in 2021 [see figure 1].

Figure 1



Source: ENISA Threat Landscape Report 2022[2]

[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

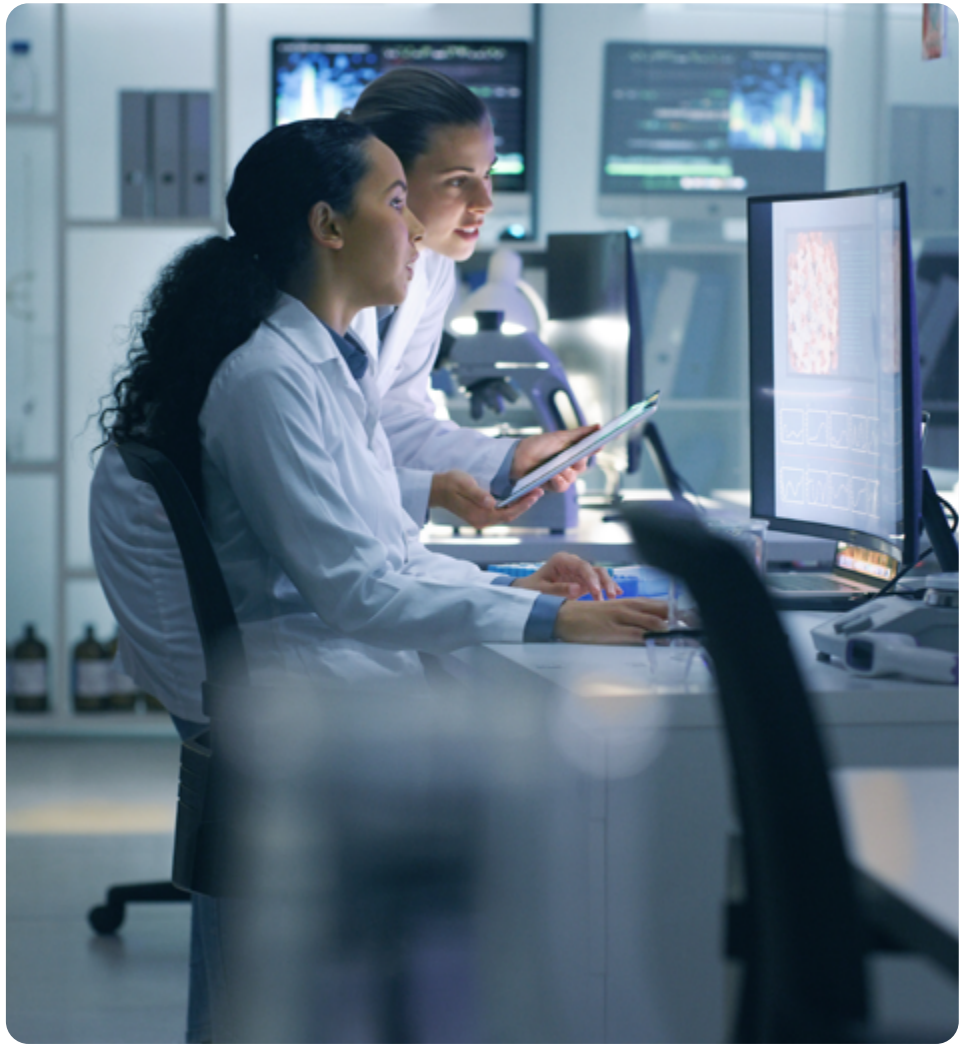
How is the impact of these cyberattacks being measured today?

Security incidents in the pharmaceutical industry can result in a broader impact, including not only financial, legal, and reputational damages, but also operational disruptions that may impact productivity and result in the loss of critical intellectual property. The Fortinet report “The 2021 State of Pharmaceuticals and Cybersecurity” highlights that pharmaceutical companies struggle to secure their intellectual property, maintain business continuity and protect mission-critical data.

98% of pharmaceutical companies reported at least one intrusion

40% of businesses experienced outages that affected productivity, safety, compliance, revenue, or brand image

28% of them lost business-critical data or IP to be transferred to other facilities



Knowing that attacks are coming is not the same as being in a position to combat them. Similarly, knowing which solutions are needed (regular patching, next-gen firewall, multifactor authentication for access management, penetration testing and so on) isn't the same as having them all deployed across networks.

Security investments need to be balanced against the clinical needs of the organization, the availability of trained IT staff, shared risk approaches with partners, the raft of compliance issues and much more.

There may be a clear and present danger, but the path to building a stout defence isn't always quite so straightforward.

2 Cybersecurity: where does responsibility rest?

In a recent interview, Ed Duryee, Columbus Regional Healthcare System's Director of Information Systems, stated that security is a board level issue, not an IT responsibility. It's a perceptive point.

While it's the CIO/CISO teams that will certainly be evaluating potential threats, selecting the cybersecurity suppliers and solutions, and managing the IT environments, the impact of a successful attack is much wider than this one department. Indeed, it goes right to the heart of patient delivery, consumer trust and to the continued operation of the facility itself.

There are the immediate financial implications of a successful attack. These range from technical remediation and clean-up costs that can stretch into millions of dollars, through to actually paying the ransom, which is not recommended by law enforcement bodies. While it's hard to get a clear picture, the cost of ransomware payments in 2019 may have been as high as €101 bn in 2019[3], with some estimates suggesting that 45% of attacked organizations paid the ransom (but half still lost their data).

Pharmaceuticals was the top 3 industry in terms of average total cost as the result of a data breach, with an estimated $5,01 million in 2022, healthcare being the highest ($10.10 million).[4] And, in many markets, the financial costs can also be felt through cancelled procedures and fines for missed targets.

[3] Ransomware, ENSIA Threat landscape, Jan 2019-Aoeril 2020
[4] IBM Cost of a Data Breach Report 2022 https://www.ibm.com/downloads/cas/3R8N1DZJ

3 Where to focus investments in 2023

There is undoubtably a need for pharmaceuticals organizations of all sizes to act, and do so in a holistic way. Increasingly, a risk-driven, zero trust strategy is the 'go-to' approach as life sciences organizations move away from point solutions into a more integrated security model. And, as we move through 2023 and beyond, the following will be the top investment priorities.

Visibility.

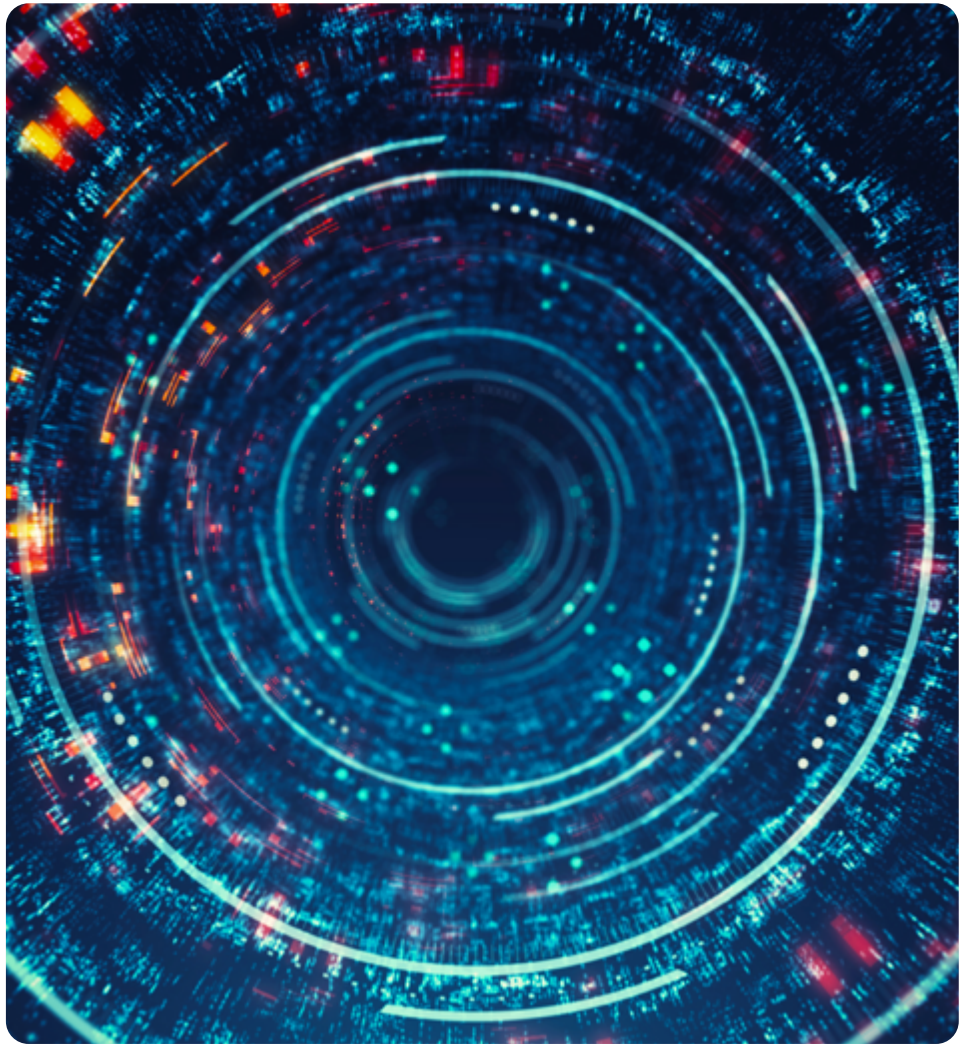
You cannot protect what you cannot see.

Organizations will invest in risk-based vulnerability management tools to improve internal visibility and enhance operational efficiency. Many successful cyberattacks exploit known vulnerabilities. Pharmaceutical companies must therefore improve their vulnerability management programs by adopting vulnerability prioritization technologies and combine them with autonomous pen-testing platforms for better results. It will also be important to invest in technologies that bring external visibility to their assets, such as digital risk protection services, cyber threat intelligence and security risk rating services.

Zero trust.

Never trust, always verify.

Pharmaceuticals will embark on (or accelerate) their zero trust journeys to reduce risk and simplify access management for staff. While there's no single path to zero trust, pharmaceuticals will focus their approach on their level of maturity. Starting with remote access and identity management of people, devices and objects will provide a solid foundation.



Hybrid cloud security.

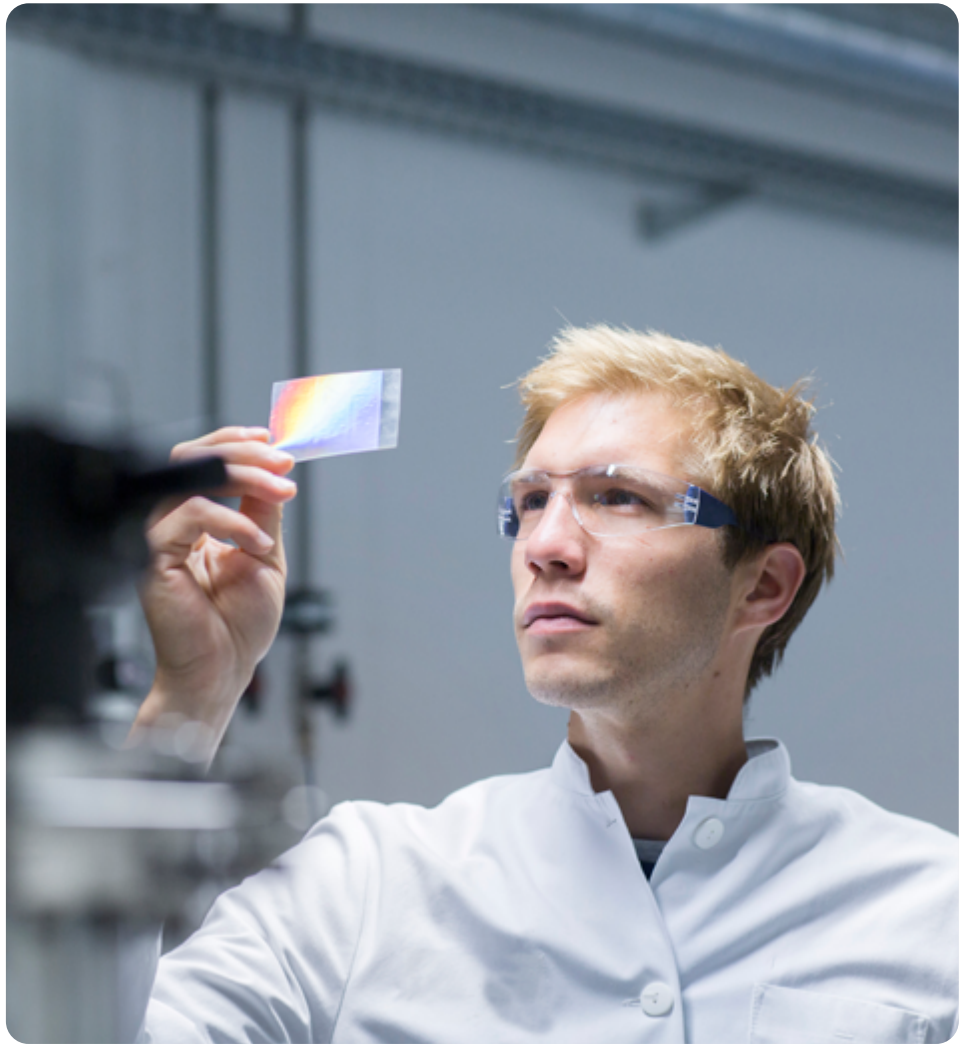
Bring trust to the cloud.

With more research and development, personal and operational data in more places, pharmaceuticals will need to implement a layer of security control across their systems. Adding a new layer of trust will secure the applications and data across multi-cloud and hybrid cloud environments, and help support compliance.

Pharma 4.0 IIoT protection.

Securing the devices that process your pharmaceutical data.

The Industrial Internet of Things (IIoT) is becoming increasingly prevalent in the pharmaceutical, biotech and meditech industry, with companies utilizing it to improve efficiency and data management across their supply chains. However, these devices can also be an entry door for hackers. It is essential to know what devices are active and inactive within your system through asset discovery and then to actively monitor, manage their lifecycle and secure them.



Managed detection and response.

Turning the tables on cyber criminals.

Managed detection and response (MDR) solutions will help anticipate and detect complex attacks using artificial intelligence algorithms to detect and orchestrate a response in near-real-time. These advanced platforms will integrate a host of applications within a single platform, including security information and event management, security orchestration automation and response, user behavioral analytics, endpoint detection response and more.

Adopt best practices.

Get the basics right

In addition to leveraging state-of-the-art security technologies above, getting the basics right around up-to-date patching, a good security hygiene, a solid backup and recovery program, staff security awareness training and fast incident response will all support a more secure healthcare environment.

4 Expert support on your journey

In this new pharmaceutical ecosystem, intellectual proprerty on patents, vaccines and drugs needs to be protected across a complex network of people, technologies and information.

This cannot be achieved by the CIO/CSO function alone and requires education of, and buy-in from, senior budget holders. Similarly, embedding appropriate level of cybersecurity is not an overnight fix or a linear journey. And, of course, it can be complex – particularly as focus shifts to deep learning and artificial intelligence technologies.

It's critical then that security solutions keep pace with the life sciences' innovation – so they can operate with complete trust. Sensitive data must be protected, but still be easily accessible, and today's increasingly connected medical devices and clinical application access points must also be protected and secured to avoid compromising the wider organization.

With a proven track record of digital compliance and cybersecurity in complex IT environments, Eviden can help pharmaceuticals do it all – while containing costs.

Connect with us

eviden.com

ECT-230612-CS-BR-Eviden-Cybersecurity-Lifescience-ebook