PERSPECTIVES

# An industry under attack – Cybercriminals target our well-being

June 2023

Cybercriminals can target both the private and public sectors [1] when exploiting vulnerabilities related to well-being, including healthcare. This broad umbrella term includes pharmaceuticals, research and many other aspects of medical care; indeed, pharmaceuticals are a vital part of healthcare but represent just one piece of the puzzle.

In the private sector, cybercriminals can target companies that offer health-related products or services, such as pharmaceutical companies or health insurance providers. They may seek to steal confidential patient information, trade secrets, or financial data. They may also launch attacks that disrupt business operations, causing harm to patients or customers.

In the public sector, cybercriminals target government agencies responsible for public health and safety, such as hospitals, public health departments, or emergency response systems. They may seek to disrupt services, steal sensitive information, or spread misinformation to cause panic and harm to the public. In 2020, the United States (US) Cybersecurity and Infrastructure Security Agency (CISA) reported increased cyberattacks targeting federal agencies, including a high-profile attack on the SolarWinds software supply chain that affected multiple government agencies. [2]

All of this means that risk-based strategies and best practices are more critical than ever. A cybersecurity breach or cybercrime can inflict mayhem on any company, compromising assets, laying bare sensitive data, and can even go so far as to result in loss of life by potentially damaging life-saving systems.

Indeed, a cybercrime could cause severe harm or even death to living organisms or critical infrastructure that supports life. Examples of such life systems that could be threatened include the human body's respiratory, cardiovascular, and nervous systems. The consequences of such events can be severe, potentially resulting in loss of life, widespread destruction, and long-lasting economic and social impacts. Therefore, it is important to respond appropriately to prevent or mitigate the effects of such events whenever possible.

A breach or cybercrime also requires time, resources, and effort to contain, eradicate and mitigate the damage. The healthcare and pharmaceutical sectors represent one area where attacks are rising.

Many industries, such as construction [3] and maritime [4] businesses, are at heightened risk from cyberattacks and cybercrimes; they are targets of choice for cybercriminals. The healthcare and pharmaceutical industry is one of the most noteworthy industries under attack as it fundamentally ensures our well-being. [5] It faces an unprecedented challenge as cybercriminals continue to target it, putting sensitive patient data and research at risk.

During 2022 and 2023, several healthcare providers, including Sharp HealthCare, Choice Health Insurance, Shields Health Care Group, and Alameda Health System, experienced data breaches with patients' personal information, such as social security numbers, health insurance data, and health records, being compromised. Moreover, the Red Cross and Red Crescent societies across the globe also suffered a complex cyberattack that resulted in the seizure of data belonging to more than 515,000 vulnerable people. [6]

*Notes*


*[1] AJ Thompson, "Public sector data under real threat from cybercriminals", Open Access Government, 11 November 2022, https://www.openaccessgovernment.org/public-sector-data-under-real-threat-from-cybercriminals/147375/*

*[2] U.S. Cybersecurity and Infrastructure Security Agency. (2021). CISA Releases Analysis Report on SolarWinds Cyber Incident. https://www.cisa.gov/news/2021/01/05/cisa-releases-analysis-report-solarwinds-cyber-incident*

*[3] Claire Mahoney, "Is the construction industry the next big cybercrime target?" Security Middle East, 29 March 2022, https://www.securitymiddleeastmag.com/is-the-construction-industry-the-next-big-cybercrime-target/*

*[4] Saiful Karim, "Study: cyber attack increase threatens sea traffic, ports and offshore rigs", riviera, 14 October 2022, https://www.rivieramm.com/opinion/opinion/study-cyber-attack-increase-threatens-sea-traffic-ports-and-offshore-rigs-73323*

*[5] "Hungary : Hungary Must Become Self-Sufficient in Life-Saving Medical Devices." MENA Report, Albawaba (London) Ltd., November 2022*

*[6] Aaron Drapkin, "Data Breaches That Have Happened in 2022 and 2023 So Far", Tech.Co, April 2023, https://tech.co/news/data-breaches-updated-list*

According to Cybersecurity Ventures, cybercrime damage is set to reach $10 trillion by 2025, making it one of the biggest threats to global businesses. [7] The World Economic Forum's Global Risks Report 2023 also highlights cyberattacks as a significant risk to the global economy, with healthcare and pharmaceutical companies among the most vulnerable. [8]

A key concern for this industry is the supply chain risk; cyberattacks on third-party vendors and suppliers can potentially compromise the entire chain. In a TechTarget Pharma News Intelligence report, the cybersecurity risk to the pharmaceutical supply chain is estimated to be over $31 million annually. [9] It is a significant concern for the industry as supply chain disruptions could have severe consequences for patients relying on life-saving medications.

Historical breaches show that the healthcare and pharmaceutical industry has always been at risk of cyberattacks as many cybercriminals aim to steal their sensitive and confidential data. This can include but is not limited to, prescriptions, research and sensitive patient information because of their valuable data; these companies have become a target of choice for cybercriminals. One type of attack method is phishing with malicious emails, including a link and message to trick the victims into clicking it, the precursor to a ransomware attack. This happened to the Texas-based OakBend Medical Center, which suffered a ransomware attack in September 2022, forcing the hospital's IT department to take all systems offline and put them in lockdown mode. [10] More recently, over 94,000 Florida Medical Clinic patients were notified that a ransomware attack deployed against the provider's network on 9 January 2023 enabled the attacker to access specific files that contained their health information. [11]

Just like in most industries, the risk of such attacks is massive for the healthcare and pharmaceutical industry. Ransomware attacks aim to extort ransom from victims using malicious software. If not paid, cybercriminals can threaten to distribute the data on the internet and often go through with it. The attack can cause companies considerable problems, such as computer downtime, financial loss and reputational damage, as evidenced by the phishing email cyber-attack that crippled the Irish Health Service Executive (HSE) in 2021. [12]

In 2022, a cyberattack on a major IT provider for the UK National Health Service (NHS) was also confirmed as a ransomware attack. [13]

Hospitals have seen variations of this type of attack. Health systems should review their cyber defences concerning webpages in response to threats from the pro-Russia hacktivist group known as Killnet, who use Denial of Service (DDoS) [14] attacks to take down forward-facing webpages and breach protected health information (PHI). [15] DDoS attacks create two primary problems for healthcare providers.

First, suppose a DDoS attack disables a hospital's forward-facing webpage, which could affect appointment scheduling, prescriptions, and other services patients access through the web portal. In that case, hospitals should prepare to conduct these administrative tasks another way.

Second, a ransomware group will conduct a DDoS attack against a target, and while the cybersecurity team deals with the attack, the group will deploy the ransomware. The cybersecurity team is focused on cleaning up DDoS attacks and does not recognise that something else is happening. The real problem arises when patient data is encrypted or stolen and leaked.

*Notes*

*[7] Steve Morgan, "Cybercrime To Cost The World $10.5 Trillion Annually By 2025", Cybercrime Magazine, November 2020, https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/*

*[8] World Economic Forum, "Global Risks Report 2023: We know what the risks are - here's what experts say we can do about it", Davos 2023, https://www.weforum.org/agenda/2023/01/global-risks-report-2023-experts-davos2023/*

*[9] Samantha McGrail, "Pharmaceutical Supply Chain Cybersecurity Risk Tops $31M Annually", TechTarget Pharma News Intelligence, 20 May 2021, https://pharmanewsintel.com/news/pharmaceutical-supply-chain-cybersecurity-risk-tops-31b-annually*

*[10] Jonathan Greig, "Texas hospital still bringing systems back online after September 1 ransomware attack", The Record, 14 September 2022, https://therecord.media/texas-hospital-still-bringing-systems-back-online-after-sept-1-ransomware-attack/*

*[11] Florida Medical Centre, "Notice of Florida Medical Clinic System Cyberattack" Press Release, March 2023, https://www.floridamedicalclinic.com/press-release/*

*[12] Colm Keena, "Opening of email attachment led to HSE cyber attack, report finds", Irish Times, 10 December 2021, https://www.irishtimes.com/news/crime-and-law/opening-of-email-attachment-led-to-hse-cyber-attack-report-finds-1.4752043*

*[13] Joe Tidy - Cyber reporter, "NHS IT supplier held to ransom by hackers", BBC News, August 2022, https://www.bbc.co.uk/news/technology-62506039*

*[14] Distributed Denial-of-Service (DDoS) Attack – it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites.*

*[15] Health Sector Cybersecurity Coordination Center, "Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector", January 2023, https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf*

The leaking of stolen data has occurred previously. Following the cyberattack on the European Medicines Agency (EMA), a decentralised agency related to the European Union responsible for reviewing and approving vaccines before distribution, monitoring, and evaluating such medicines, cybercriminals leaked Covid-19 vaccination data from Pfizer and BioNTech. [16]

It is imperative for pharmaceutical and healthcare providers to be aware of the threats to the industry and to have a plan and the right technology in place to identify and mitigate them.

Automation, third-party sellers, vendors, healthcare groups and new technological tools dominate the healthcare and pharmaceutical industry. They are beneficial, as they are needed to maintain vital supply chains and support research, care and development. However, if a third-party vendor is breached, it can damage all its partners. What is more, third-party access and security within healthcare are at significant risk. [17] This was evidenced in July 2022, when Infinity Rehab notified the US Department of Health and Human Services (HHS) that 183,254 patients had stolen their personal data. At the same time, Avamere Health Services informed the HHS that 197,730 patients had suffered a similar fate. Then on 16 August, Washington's MultiCare revealed that 18,165 more patients were affected in the same breach. [18]

Additionally, introducing the Internet of Things (IoT) in the healthcare and pharmaceutical industry makes it vulnerable to cyberattacks and cybercrimes. They use IoT to streamline and analyse critical patient data while multifaceted procedures are becoming more effective. While IoT devices are firmly associated with the industry [19], they increase cyberattack vectors due to vulnerabilities. [20]

Many companies associated with or within the industry have merged or been acquired by giant corporations. This can harm cybersecurity because subsidiary companies tend not to invest in their security frequently; thus, the well-protected parent companies can find their security compromised. Therefore, companies should proactively prioritise their cybersecurity and cybercrime prevention before taking the necessary acquisition actions.

When organisations take a prevention-first approach to their inclusive business decisions, they will be better positioned to manage and monitor cyber risks proactively rather than react and recover after an attack or cybercrime. [21]

Preventative and active protection can address these cybersecurity challenges and offer the healthcare and pharmaceutical industry powerful protection against cybercrime and insider threats. To address cybersecurity challenges, healthcare and pharmaceutical companies must proactively approach cybersecurity and implement preventative measures to protect sensitive data. [22] This can include securing the network perimeter, managing privileged access, implementing a zero-trust network access approach, and securing cloud environments. Cybersecurity and cybercrime prevention training should also be provided to employees to minimise the risk of insider threats.

A cyber gap and impact assessment can identify the risks that are present. Such an evaluation would include the digital and real world to identify any voids that malicious attackers could use knowingly or unknowingly. Once known, the organisation can use its risk appetite to deal with, pay to remove them, introduce compensating measures and controls, or accept the risk.

In conclusion, every industry needs strong cybersecurity and cybercrime prevention to protect its data and vital information from cybercriminals. Especially as companies, healthcare and pharmaceutical are desirable targets for cybercriminals. These companies should take the appropriate steps, identify the risks, make decisions, and implement solutions and best practices to protect themselves. They have an overabundance of confidential data, which, if breached, can cause grave consequences and potentially harm the economy, health and the public in general. By taking a proactive approach, the industry can protect sensitive data and mitigate the risk of significant financial and reputational damage.

*Notes*

*[16] Caleb Townsend, "Pfizer/BioNTech COVID-19 Vaccine Data Leaked by Hackers", United States, Cybersecurity Magazine, 2021, https://www.uscybersecurity.net/cyberNews/pfizer-biontech-covid-19-vaccine-data-leaked-by-hackers/*

*[17] In Collaboration with SecureLink, "Third-party risk in healthcare: a continuing crisis", 30 September 2022, Becker's Health IT, https://www.beckershospitalreview.com/cybersecurity/third-party-risk-in-healthcare-a-continuing-crisis.html*

*[18] DataBreaches.net, "Infinity Rehab and Avamere Health Services notify 380,984 patients about breach at Avamere (with updates)", July 2022, https://www.databreaches.net/infinity-rehab-and-avamere-health-services-notify-380984-patients-about-breach-at-avamere/*

*[19] Kimberly Gregorio, "6 Real-World Opportunities & Use Cases for IoT in the Pharma Industry", birdzai, 25 February 2022, https://www.p360.com/birdzai/6-real-world-opportunities-and-use-cases-for-io-t-in-the-pharma-industry/*

*[20] Florida Medical Centre, "Notice of Florida Medical Clinic System Cyberattack" Press Release, March 2023, https://www.floridamedicalclinic.com/press-release/*

*[21] McKinsey & Company "Cybersecurity trends: Looking over the horizon", McKinsey & Company article, 10 March 2022, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon*

*[22] Laiba Siddiqui, "Command and Control: Understanding & Defending Against C2 Attacks", Splunk, 31 March 2023, https://www.splunk.com/en_us/blog/learn/c2-command-and-control.html*

## Contacts


**Darren Mullins**
Partner
darren.mullins@accuracy.com
+971 56 682 5681

**Paul Wright**
Senior Adviser
paul.wright@accuracy.com
+971 522 449429

**Arthur Couvreur**
Director
arthur.couvreur@accuracy.com
+33 6 66 69 65 15

**Steve Molloy**
Director
steve.molloy@accuracy.com
+39 334 10 49 578


*Accuracy partners and professionals are available to discuss your needs and design an appropriate solution with the relevant experts.*