KnowBe4

Hacked Healthcare:

A Global Crisis in Cybersecurity

HACKED HEALTHCARE: A GLOBAL CRISIS IN CYBERSECURITY

If you have not experienced a cyberattack on a hospital, you have probably heard about it: ambulances with patients in crisis being sent away, surgeons and oncologists losing access to electronic health records, phone systems and systems used to order tests, procedures, and medications crashed, and the portal that allows patients to communicate to their providers inaccessible. Doctors and nurses are often forced to revert to paper records without the information needed to do their jobs. Non-emergency surgeries, tests and appointments are paused. Emergency cases are triaged.

Hospital groups, which are becoming more frequent targets of ransomware attacks, may see millions of visitors each year. The impact of an attack can be staggering. Hospitals are often forced to treat fewer patients. Those they do treat receive fewer services. Doctors make diagnoses without imaging; nurses may be unable to monitor the vital signs of patients in an intensive care unit (ICU) when they are not physically in the room.

Cyberattacks against hospitals are not white-collar crime. They can result in loss of life. In October 2023, researchers at the University of Michigan School of Public Health released findings from a five-year study showing that in-hospital mortality significantly increased during such attacks, in part due to a 17%-25% drop in hospital admissions. The study found that between 2016 and 2021, cyberattacks and the resulting disruption may have contributed to the deaths of 42 to 67 patients.[1]

To illustrate, CNN recently interviewed nurses at two hospital locations that had suffered ransomware attacks in the previous three weeks. When nurses were forced to manually enter prescription information and work without electronic health records, one said that it was "putting patients' lives in danger" and that medical staff "have too many patients for what is safe." Another nurse said that "It is frightening how many safety guardrails [have been] out of service without any computers."[2]

1 McGlave, Claire and Neprash, Hannah and Nikpay, Sayeh, Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients (October 4, 2023). Available at SSRN: https://ssrn.com/abstract=4579292 or http://dx.doi.org/10.2139/ssrn.4579292

2 Lynngaas, Sean, "'It's putting patients' lives in danger': Nurses say ransomware attack is stressing hospital operations," May 29, 2024, CNN, https://www.cnn.com/2024/05/29/tech/ransomware-attacks-hospitals-patients-danger/index.html

Timeline

December

On the morning of December 24, 2023, emergency care operations at three hospitals in Germany were disrupted following a ransomware attack. The hospitals impacted were Franziskus Hospital Bielefeld, Mathilden Hospital Herford, and Sankt Vinzenz Hospital Rheda-Wiedenbruck.[1]

January

On January 4, 2024, it was reported that class action lawsuits were filed against Texas-based ESO Solutions over a cyberattack to the software manufacturer that affected almost 2.7 million individuals and included the theft of sensitive medical records. The attack occurred in October 2023 2024, and impacted 14 hospitals in the U.S. The lawsuits allege that ESO Solutions failed to implement reasonable and appropriate industry-standard security measures to ensure the privacy and confidentiality of patient data, and that the company did not properly train staff members on data security protocols, failed to detect a breach of its systems and the theft of data in a timely

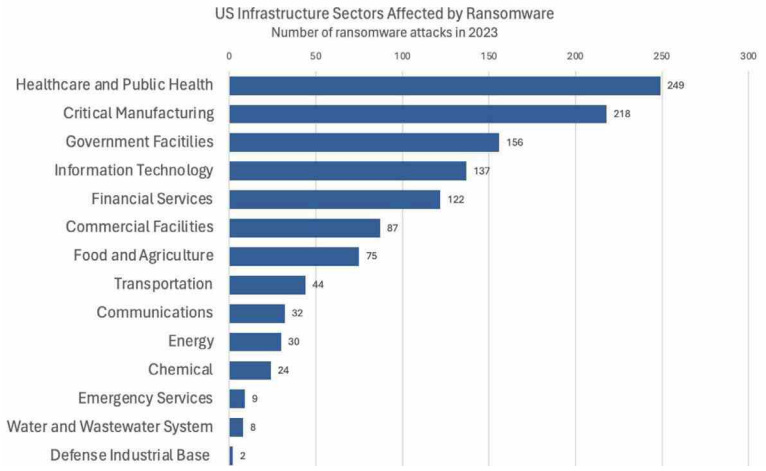
1 "Hospitals targeted by LockBit ransomware attack in Germany," SC Media, December 28, 2023, https://www.scmagazine.com/brief/german-hospitals-targeted-by-lockbit-ransomware-attack

The wave of attacks is growing, not receding. In May 2024, after an attack on a group of 140 hospitals, the Health-ISAC (Health Information Sharing and Analysis Center), published an advisory warning that hackers using ransomware have "recently accelerated attacks against the healthcare sector." The warning cited two healthcare organizations in Europe and another in the U.S. that had "suffered severe operational disruptions" just in the previous month. John Riggi, AHA's national advisor for cybersecurity and risk, recommended that the alert "be reviewed with high urgency."[3]

THE 2023 PICTURE

> ***"...attacks in the global healthcare sector outpaced the global average by more than four times, with an average of 1613 attacks per week."***

According to Check Point Research, in the first three quarters of 2023, there was a 3% uptick in average weekly global cyberattacks compared to the corresponding period in the previous year—not enough to set off alarms. But attacks in the global healthcare sector outpaced the global average by nearly four times, with an average of 1,613 attacks per week—an 11% year-over-year surge that is still rising.[4]



3 "Agencies warn of accelerating attacks on health care by Black Basta ransomware group," American Hospital Association, May 10, 2024, https://www.aha.org/news/headline/2024-05-10-agencies-warn-accelerating-attacks-health-care-black-basta-ransomware-group

4 "A Continuing Cyber-Storm with Increasing Ransomware Threats and a Surge in Healthcare and APAC region," Check Point Research, October 25, 2023, https://blog.checkpoint.com/security/a-continuing-cyber-storm-with-increasing-ransomware-threats-and-a-surge-in-healthcare-and-apac-region/

manner, and then failed to issue timely notifications to the affected individuals. The lawsuits also allege that the data security failures violate the Health Insurance Portability and Accountability Act (HIPAA).[2]

On January 25, 2024, the computer system of the Canadian Capital Health Communication Center (CCSC) suffered a ransomware attack that affected the entire ambulance system of the Capitale-Nationale region, Saguenay-Lac-St-Jean and Nord-du-Québec. With the computer system that allows paramedics to locate calls completely paralyzed, Frédéric Maheux, president of the Association of Prehospital Workers (ATPH) described the scene as "total panic on the roads" as paramedics used their own phones to find their way around the city and get to the scene of calls. The attack was caused by a person on the administrative networks activating a fraudulent (phishing) email.[3]

On January 27, 2024, Instituto Nacional do Câncer (INCA) in Brazil, was hit by a cyberattack that disrupted the radiotherapy area and appointment scheduling.

2 Alder, Steve, "Class Action Lawsuits Filed Against ESO Solutions Over Data Breach," The HIPPA Journal, January 4, 2024

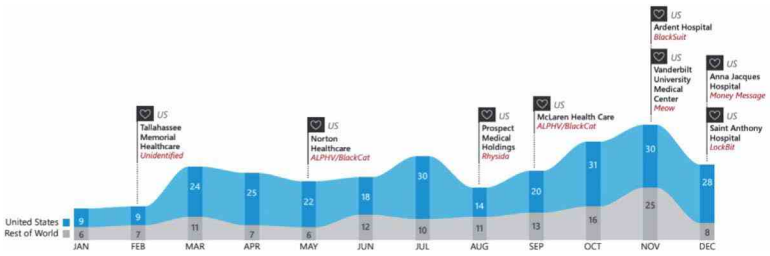
3 Baril, Victoria, "Hackers attack ambulance services," The Sun, January 25, 2024, https://www.lesoleil.com/actualites/justice-et-faits-divers/2024/01/25/des-pirates-sen-prennent-aux-services-ambulanciers-JTIY6MSQNVDFJKCF2YOWJ5QDUE/

IC3, the Federal Bureau of Investigation's Internet Crime Complain Center, logged 2,825 complaints identified as ransomware in 2023. These included attacks against 16 U.S. critical infrastructure sectors. In keeping with global trends, healthcare and public health stood out as the most frequently attacked sector:

https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf

In a study of 6,100 organizations across its customer base and 1,600 IT and security leaders, Rubrik Lab Zero in Palo Alto found that globally, healthcare organizations experienced 50% more encryption events than the global average across 2023.[5]

The U.S. Department of National Intelligence echoed the trend, noting that globally, ransomware attacks against the healthcare sector steadily increased and nearly doubled in 2023. In the U.S. alone, attacks against healthcare institutions more than doubled, with a 128% increase.[6]



RANSOMWARE ATTACKS ON HEALTHCARE RISING WORLDWIDE IN 2023

Cyberattacks against healthcare institutions are also surging in costs. IBM's 2023 Cost of a Data Breach Report[3] showed the global average cost of a data breach reached $4.45 million in 2023 – an all-time high for the report and a 15% increase over the last three years. Both the rate of increase in costs per attack for the sector in the last three years, and the average cost of a breach, were more than three times higher than the global average in the same period, with the cost per breach in healthcare averaging nearly $11 million, the costliest of all sectors.

5 "The State of Data Security: Measuring Your Data's Risk," Rubric Lab Zero, April 30, 2024, https://www.rubrik.com/company/newsroom/press-releases/24/healthcare-organizations-lose-sensitive-data-in-every-ransomware-attack

6 "Ransomware Attacks Surge in 2023," Department of National Intelligence, February 28, 2024, https://www.dni.gov/files/CTIIC/documents/products/Ransomware_Attacks_Surge_in_2023.pdf

Scheduled consultations continued with manual records, but booking new appointments was suspended.[4]

On January 29, 2024, the Middle Franconia District Hospitals in the Ansbachof Germany fell victim to a cyberattack that encrypted and stole patient data. Emergency services were halted. Most of the hospitals in the network could only be reached by telephone, and the hospital at Europakanal in Erlangen was unable to make calls.[5]

On January 31, 2024, Caritas Dominikus Clinic in Berlin was the victim of a cyberattack that resulted in the telephone system being taken offline; an emergency telephone number was temporarily set up while emergency patients were diverted. The attack is not believed to have resulted in a data breach.

On January 31, 2024, Lurie Children's Hospital in Chicago suffered a ransomware attack from the Rhysida ransomware group that took the institution's entire computer network offline and forced staff to resort

4 "Overview of cyber attacks in week 5/2024," Computer Weekly.de, February 5, 2024, https://www.computerweekly.com/de/news/366568753/Die-Cyberangriffe-der-KW5-2024-im-Ueberblick

5 "Hacker attack on district hospitals in Middle Franconia,' BR24, January 29, 2024, https://www.br.de/nachrichten/bayern/hackerangriff-auf-bezirkskliniken-mittelfranken,U2jU9a2

"Both the rate of increase in costs per attack for the sector in the last three years, and the average cost of a breach, were more than three times higher than the global average in the same period."

AVERAGE COST OF A DATA BREACH (IBM COST OF A DATA BREACH REPORT, 2023):

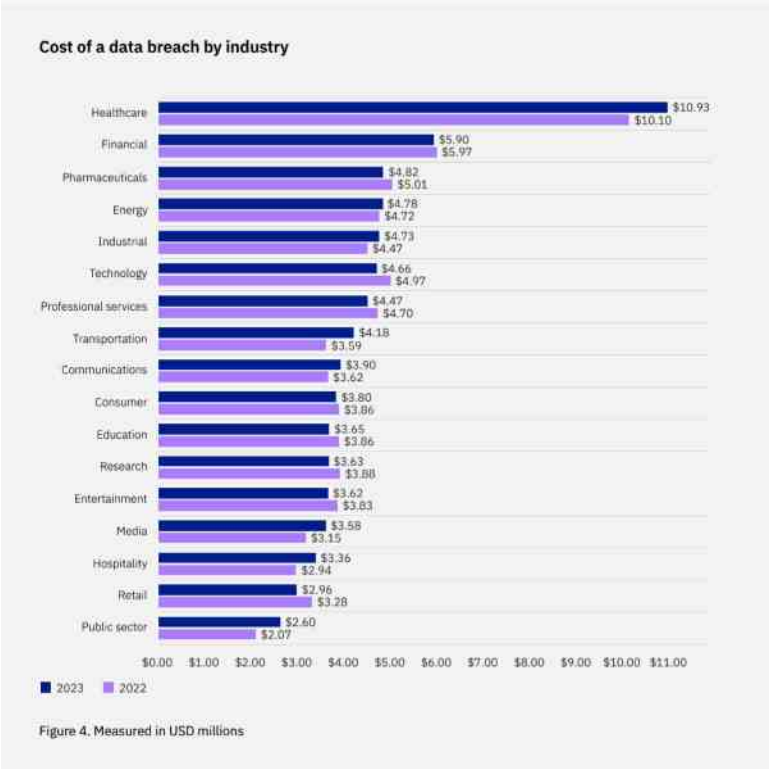


Figure 4. Measured in USD millions

THE ATTRACTIVE TARGET

There are three primary factors that make the global healthcare sector a particularly attractive target for cybercriminals:

Sensitivity and potential value of the information. Medical records provide one of the most complete collections of personal information for any given individual, including not only financial and insurance information, but to manual processes. Lurie Children's Hospital provides care to more than 239,000 children annually across its downtown Chicago hospital, 17 outpatient service locations and six primary care sites. On March 7, 2024, the ransomware group claimed to have sold data stolen from the hospital after listing it on the dark web for $3.4 million. The listing was updated to claim: "All data was sold." It came just as the hospital announced it was making progress restoring its key systems, including its electronic health record platform and its phone system.[6]

February:

On February 2, The Armentières hospital in France suffered a cyberattack that brought their system down, accompanied by a ransom demand. The emergency room was closed, and new patients were being redirected to other hospitals.[7]

6 Martin, Alexander, "Ransomware gang claims to have made $3.4 million after attacking children's hospital," The Record, March 7, 2024, https://therecord.media/ransomware-gang-claims-payment-luries

7 "Armentières hospital victim of cyber attack, emergency rooms closed for the day," February 2, France Blue, https://www.francebleu.fr/infos/sante-sciences/l-hopital-d-armentieres-victime-d-une-cyber-attaque-les-urgences-fermees-pour-la-journee-5946592

family relationships, diagnoses and treatments, records that could be considered "compromising" such as nude photos of a patient in treatment for breast cancer, records of domestic violence, or notes and conclusions of a psychotherapist or psychiatrist.

In its April 2024 report, Rubrik Lab Zero gives a clearer picture of the sheer volume of sensitive information held by healthcare institutions:

- Healthcare organizations secure 22% more data than the global average.
- A typical healthcare organization saw their data estate grow by 27% in 2023.
- A typical healthcare organization has more than 42 million sensitive data records — 50% more sensitive data than the global average.
- Sensitive data records in observed healthcare organizations grew by more than 63% in 2023—far surpassing any other industry and more than five times the global average (13%).
- Ransomware attacks against observed healthcare organizations have an estimated impact of almost five times more sensitive data than the global average.[7]

There is a higher liability to patients from having their personal health data exposed compared to an exposed credit card number or password. If your credit card information gets stolen by a hacker, you can cancel and replace the card. If your password is compromised, you can change it. But an individual's medical information cannot be changed; once exposed, it is on the dark web virtually permanently.

In the eyes of a cybercriminal, these factors, coupled with the potential loss of life resulting from an attack, make it more likely that a hospital will pay a ransom to protect its patients. If not, the stolen information still has high value; there is a huge global black market for health records, which can be maliciously used for identity theft, insurance fraud, blackmail, surveillance, and more, making the individual pieces of data more valuable. On the dark web, medical records sell for $60 compared to $15 for a Social Security number and $3 for a credit card.[8]

7 "The State of Data Security: Measuring Your Data's Risk," Rubric Lab Zero, April 30, 2024, https://www.rubrik.com/company/newsroom/press-releases/24/healthcare-organizations-lose-sensitive-data-in-every-ransomware-attack

8 Caminiti, Susan, "Why UnitedHealth, Change Healthcare were targeted by ransomware hackers, and more cybercrime will hit patients, doctors," CNBC, March 15, 2024, https://www.cnbc.com/2024/03/15/why-unitedhealth-change-healthcare-were-targets-of-ransomware-hackers.html

Also on February 2, 2024, a breach of French healthcare payment services Viamedis and Almerys resulted in the theft of data on more than 33 million people; stolen information included customers' 'medical data and their family's personal information. It is the largest cyberattack in French history. The company serves 20 million insured individuals through 84 healthcare organizations. The attack began with a phishing email.[8]

On February 5, 2024, a cyberattack on the website of the Provincial Health Authority of Cosenza (ASP) in Italy disrupted essential services including appointments, online consultations and records on vaccinations and healthcare services, slowing emergency services and other care. The security of sensitive information was compromised.[9]

On February 9, 2024, a cyberattack paralyzed IT systems at Lindenbrunn Hospital In Lower Saxony, Germany. The attack affected both facilities of

8 Stewart, Ellis, "Half of France's Data Swiped in Viamedis and Almerys Cyber Attack," EM 360, December 2,, 204, https://em360tech.com/tech-article/viamedis-almerys-cyber-attack

9 "Hacker attack on the Cosenza ASP website: the provision of services blocked," February 5, 2024, Calabria Diretta News, https://www.calabriadirettanews.com/2024/02/05/attacco-hacker-al-sito-dellasp-di-cosenza-bloccata-lerogazione-dei-servizi/

Interconnectedness. Hospitals are among the most digitally connected places in the world. Advances in equipment have created a constant flow of information, from diagnostic tools such as MRIs to robotic surgery to doctor's notes on visits and results, to patient portals on computers at home and on handheld devices, and much more.

The digital river of information goes well beyond hospitals and health clinics. It can include biotechnology companies or academic research institutions running trials, vaccine manufacturers, pharmaceutical companies and pharmacies filling prescriptions, diagnostic laboratories, health IT suppliers, digital infrastructure vendors and medical device manufacturers. All of these organizations have been targeted by cyberattacks.

The growing field of IoHT, or Internet of Health Things (sometimes referred to as IoMT, the Internet of Medical Things) promises to expand this interconnectedness exponentially, with physical devices embedded in patients with electronics and sensors, and network connections. These will include ingestible sensors, i.e. pill-sized devices for collecting and tracking information like stomach pH, temperature, enzymes, etc., and further sophistication of handheld devices enabling patients to view their medical data in real time.

"Advances in digital solutions in healthcare have… created digital dependence, which is often advanced without comparable investment in cybersecurity."

Poor security. Advances in digital solutions in healthcare have enhanced both the quality and the cost-efficiency of health services. They have also created digital dependence, which is often advanced without comparable investment in cybersecurity.

Modern and increasingly fast-evolving digital technology produces new IT systems that often do not easily integrate into hard-to-replace legacy systems. This is particularly true in smaller hospitals and doctors' practices that often do not have the money, know-how, or IT staff to revamp their systems. At hospitals of all sizes, money will be spent on the latest MRI technology or additional staff far more easily than on digital protections.

the Lindenbrunn Health and Care Facility Association (GP). A ransom demand was received. The extent of the attack and whether data was affected is currently still unclear.

On February 13, 2024, over one hundred hospitals in Romania were taken offline by a ransomware attack. Romanian cyber officials said the hospital's data had recently been backed up, reducing the impact. 24 facilities, primarily children's hospitals and emergency services were directly impacted; an additional 79 hospitals were taken offline as a precaution, crashing the systems for booking, medical records, imaging equipment, and more.[10]

On February 19, 2024, HAL Allergies in the Netherlands, a leading company in the development, production, and distribution of allergen immunotherapies, was hit with a second cyberattack by Black Cat/AlphV, now renamed RansomHouse. The network was brought down resulting in delayed shipments. On February 29, 2024, RansomHouse posted on the dark web that they had exfiltrated 105GB of data from the company, with evidence.[11]

---

10 Valance, Chris, and Tidy, Joe, "Ransomware attack hits dozens of Romanian hospitals," BBC, February 13, 2024, https://www.bbc.com/news/technology-68288150

11 HackManiac on X.com, "Cyber Attack Alert," February 29, 2024, https://x.com/H4ckManac/status/1763089138893406497/photo/1

THE CHANGING LANDSCAPE

For many years, cybercrime was white collar crime, financially motivated and deployed by opportunist hackers who for the most part considered hospital and other life-threatening attacks "off limits." In recent years, as organized criminal gangs and military units have replaced rogue, individual hackers as the primary perpetrators of cyberattacks, hospitals have moved up the list of attractive targets. In some cases, the threat to public health and safety is not a byproduct. It is part of the plan.

"The bulk of the perpetrators of highly damaging healthcare attacks are located in countries where the governments at best turn a blind eye, and at worst facilitate attacks or use the perpetrators for intelligence value in exchange for impunity."

The bulk of the perpetrators of highly damaging healthcare attacks are located in countries where the governments at best turn a blind eye, and at worst facilitate attacks or use the perpetrators for intelligence value in exchange for impunity. Some, such as North Korea, use attacks as a means to finance the government and bypass sanctions. As the vast majority of the attackers operate in safe havens where criminals, even when caught, will not be extradited or punished, law enforcement efforts on the part of the nations suffering the attacks have been largely ineffectual in stemming the tide.[9]

Another sign of ransomware's increased sophistication is its relative effectiveness rate—ransomware accounted for more than 70 percent of the successful cyberattacks on healthcare organizations over the past two years.

On February 21, 2024, a cyberattack knocked Change Healthcare—a subsidiary of the behemoth global health company UnitedHealth—offline for a month, which created a backlog of unpaid claims. Change Healthcare, one of the largest health payment processing companies in the world acts as a clearing house for 15 billion medical claims each year—accounting for nearly 40 percent of all claims. The attack left doctors' offices and hospitals with serious cashflow problems, threatening patients' access to care.

It has since come to light that millions of Americans, perhaps as high as 1 in 10 Americans, may have had their sensitive health information leaked onto the dark web, despite UnitedHealth paying a $22 million ransom to the cyberattackers. Particularly hard hit were community health clinics that serve more than 30 million poor and uninsured patients.

In total, the attack cost UnitedHealth a staggering $1.6 billion as a result of the attack, nearly $600 million of that spent on system restoration and response efforts, the rest in lost revenue and business interruption.[12]

9 Riggi, John, "Ransomware Attacks on Hospitals Have Changed," May 15, 2020, American Hospital Association, https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed

12 Leo, Leroy and Roy, Sriparna, "UnitedHealth to take up to $1.6 billion hit this year from Change hack," Reuters, April 16, 2024, https://www.reuters.com/business/healthcare-pharmaceuticals/unitedhealth-warns-115-135share-hit-this-year-hack-2024-04-16/

THE 2024 SNAPSHOT:

NORTH AMERICA

The IBM X-Force Threat Intelligence Index 2024 notes that, across sectors, 50% of global cybersecurity incidents reported in 2023 took place against institutions in North America, with 86% of those happening in the United States and just 14% in Canada. Healthcare was the third most targeted sector, accounting for 15% of all incidents.

Statistics from the U.S. Department of Health and Human Services are more dramatic; according to its figures, there were over 630 ransomware incidents impacting healthcare worldwide in 2023; more than 460 of these, or 73%, affected the U.S. Health and Public Health sector.[10]

The dramatic increase in cyberattacks has prompted the U.S.'s top health agency, The Department of Health and Human Services (HHS), to develop new rules for hospitals to protect themselves from cyber threats. The HHS has said it will rewrite the rules for the Health Insurance Portability and Accountability Act—the federal law commonly called HIPAA that requires insurers and health systems to protect patient information – to include new provisions that address cybersecurity later this year.

The department is also considering new cybersecurity requirements attached to hospitals' Medicaid and Medicare funding.[11]

"The more prepared we are the better," said Deputy Secretary for the HHS Andrea Palm. But, she added, some hospitals will struggle to protect themselves. She is worried about rural hospitals, for example, that may have difficulty cobbling together money to properly update their cybersecurity.[12]

10 "Threat Assessment: BianLian," January 24, 2024, Palo Alto Network Unit 42, https://unit42.paloaltonetworks.com/bianlian-ransomware-group-threat-assessment/

11 "Healthcare Sector Cybersecurity," Department of Health and Human Services, December, 2023, https://aspr.hhs.gov/cyber/Documents/Health-Care-Sector-Cybersecurity-Dec2023-508.pdf

12 Associated Press, "Cyberattacks on Hospitals Are Likely to Increase, Putting Lives at Risk, Experts Warn," February 14, 2024, https://www.usnews.com/news/us/articles/2024-02-14/cyberattacks-on-hospitals-are-likely-to-increase-putting-lives-at-risk-experts-warn

March:

On March 2, 2024, there was a cyberattack on the IT infrastructure of the Trinity Hospital in Lippstadt in the Soest district of Germany that also affected associated hospitals the Marien Hospital Erwitte and the Hospital zum Heiligen Geist Geseke. No new admissions or planned surgeries could be performed.

On March 19, 2024, Goed, a healthcare retailer in Belgium, fell victim to a cyberattack that resulted in stolen data, all systems being disconnected, prescriptions unable to be filled, and payment processing down. Investigations are reportedly ongoing to determine whether patients'' personal information was stolen during the attack. The healthcare retailer has pharmacies (about 90) and home care stores (about 35). The store sells and rents health aid to support patients staying at home and is part of the Belgian health insurance provider CM.[13]

On March 15, 2024, the National Health Service for Dumfries and Galloway, part of the Scottish healthcare

13 Herijgers, Laura, "Care retailer of Belgian health insurance provider victim of data breach," April 17, 2024, TechZine Magazine, https://www.techzine.eu/news/security/117935/care-retailer-of-belgian-health-insurance-provider-victim-of-data-breach/

EUROPE

In July 2023, the European Union Agency for Cybersecurity (ENISA) published the results of its first-ever analysis of the cyber threat landscape of the health sector in the European Union (EU). The report maps healthcare cyber incidents between January 2021 and March 2023, studying 99 incidents and identifying the key targets of attacks, the threat actors behind them, and the impact of the attacks.

EU healthcare providers (53% of the total incidents), and especially hospitals (42%) were the most heavily affected institutions in the report. It also observed incidents targeting health authorities, bodies and agencies (14%) and attacks on the pharmaceutical industry (9%).

Ransomware was noted as one of the prime threats in the health sector (54%), both in the number of incidents but also in its impact on health organizations, something the report noted was expected to continue as a trend. It noted that 43% of ransomware incidents are coupled with a data breach or data theft, while operational disruptions are the other common effect of the attacks. It noted that almost half of total incidents (46%) were a form of threat against the data of health organizations, saying "Data related threats continue to be one of the main threats in the sector, not only for Europe but also globally."

The ENISA report also noted that despite the extent to which ransomware was used in attacks, 27% of healthcare organizations did not have a dedicated ransomware defense program. The study also revealed a lack of security awareness training for non-IT staff, with only 40% of original equipment suppliers providing security awareness training to non-IT staff.[13]

UNITED KINGDOM

In 2021, Obrela Security Industry noted in its Digital Universe Report that a staggering four-fifths (81%) of UK healthcare organizations had detected an attempted ransomware attack against their organizations in the previous year. A survey of 100 cybersecurity managers in the health sector also found that 38% of UK healthcare organizations have elected to pay a ransom demand to get their files back; 44% revealed they had refused to pay a demand but lost their healthcare data as a result.[14] In 2022, attacks in the public sector in the UK rose another 77%.[15]

13 "ENISA Threat Landscape: Health Sector," European Union Agency for Cybersecurity, July 2023, https://www.enisa.europa.eu/publications/health-threat-landscape

14 Coker, James, "81% of UK Healthcare Organizations Hit by Ransomware in Last Year," October 20, 2021, Info Security Magazine, https://www.infosecurity-magazine.com/news/healthcare-ransomware-last-year/

15 "Check Point Research Reports a 38% Increase in 2022 Global Cyberattacks," Check Point Research, January 5, 2023, https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/

system, announced that it had suffered "a focused and ongoing cyberattack." The institution, which serves just under 150,000 people, warned in the announcement that "hackers have been able to acquire a significant quantity of data."

On March 29, 2024, the group, which calls itself INC Ransom, published some of what it claims are terabytes of data exfiltrated from the organization as evidence. The data posted included clinical data. INC Ransom is threatening to release more data unless the ransom is paid by the health board.[14]

April:

On April 1, 2024, NorthBay Health near Sacramento, California, suffered a ransomware attack that resulted in patients being turned away, phone systems and imaging equipment being down, and an inability to schedule appointments. NorthBay Health operates NorthBay Medical Center in Fairfield, NorthBay VacaValley Hospital in Vacaville, three primary care facilities—two in Fairfield and one in Vacaville—and numerous specialty care offices in both cities near Sacramento, California.[15]

14 Martin, Alexander, "Ransomware gang leaks stolen Scottish healthcare patient data in extortion bid," March 29, 2024, The Record, https://therecord.media/healthcare-ransomware-data-breach-nhs-scotland

15 Sarfaty, Cheryl, NorthBay Health falls victim to cyberattack," North Bay Business Journal, April 15, 2024, https://www.northbaybusinessjournal.com/article/industrynews/cyberattack-northbay-health-solano-county/

It was not letting up by July 2023, when TechCrunch reported on an attack on Barts Health National Trust, saying that "The U.K.'s largest [National Health Service] trust has confirmed it's investigating a ransomware incident as the country's public sector continues to battle a rising wave of cyberattacks." Barts Health NHS Trust runs hospitals in London serving more than 2.5 million patients. The Black Cat/ALPHV ransomware gang claimed responsibility for the attack, claiming to have stolen 70 terabytes of sensitive data in what it claims is the biggest breach of healthcare data in the United Kingdom. Samples of the stolen data, seen by TechCrunch, include employee identification documents, including passports and driver licenses, and internal emails labeled "confidential."[16]

Asia-Pacific (APAC)

Trend Micro reported in 2022 that the "Agenda" ransomware, customized ransomware written in the Go language, a high-level programming language developed at Google, was being used to target healthcare and education organizations in Indonesia, Thailand, Saudi Arabia, and South Africa. After appearing to go dormant in 2022, it was noted as a rising threat again in October 2023.[17]

On December 7, 2023, Mr. Ivo Peixinho, head of cybercrime intelligence at Interpol, told his audience at the ISC2 Secure Asia-Pacific forum that while in the past ransomware attacks have primarily targeted money-related sectors such as professional services, information technology, manufacturing and construction, they are shifting toward healthcare.

"But we see healthcare there... We are seeing a shift in attacks on critical infrastructure, which is very concerning and catches our eye," he said, adding that the world will see more physical implications from ransomware as the frequency and scale of attacks become more apparent.

Mr. Peixinho's words echoed those of Singapore Health Minister Ong Ye Kung speaking to the Parliament just a little over two weeks earlier, where he said that attacks on healthcare were on the rise. He added that Singapore's national healthcare IT provider Synapxe receives and blocks an average of 3,000 malicious emails per day, and 1.7 million attempts to bypass Internet-facing firewalls per month.[18]

16 Page, Carly, "UK battles hacking wave as ransomware gang claims 'biggest ever' NHS breach," July 10, 2023, TechCrunch.com, https://techcrunch.com/2023/07/10/uk-hacks-public-sector-nhs-ransomware/

17 Tredger, Christopher, "Agenda ransomware threatens to resurface," IT Web, October 3, 2023, https://www.itweb.co.za/article/agenda-ransomware-threatens-to-resurface/JBwErvn3RdQ76Db2

18 Wong, Andrew, "Criminals shifting focus to target healthcare infrastructure for ransomware attacks: Interpol," The Straits Times, December 7, 2023, https://www.straitstimes.com/singapore/courts-crime/criminals-shifting-focus-to-target-healthcare-infrastructure-for-ransomware-attacks-interpol

On April 2, 2024, Nottingham Rehab Supplies (NRS) Healthcare, which supplies health and care equipment across the UK, suffered a ransomware attack and the NRS website was taken offline. The company said it is currently in its "recovery phase" following the incident; investigations are still in progress.

A number of UK local authorities, including East Lothian Council, Waltham Forest Council, Camden Council in London, Buckinghamshire Council, and Oxfordshire County Council, have now revealed that NRS has informed them that personal data of residents may have been breached by the attackers. Additional specifics have not been reported, meaning the data has been in the hands of the attackers for many weeks without those affected being notified.[16]

While still recovering from the February attack, Change Healthcare was attacked a second time; in early April 2024, a ransomware group called RansomHub posted to its dark-web site that it has four terabytes of data stolen from Change, that they will sell if a new ransom is not paid. The group claims to be unaffiliated with Black Cat/AlphV, the perpetrators of

16 Coker, James, "UK Councils Warn of Data Breach After Attack on Medical Supplier," Info Security Magazine, May 17, 2024, https://www.infosecurity-magazine.com/news/uk-councils-data-breach-medical/

Ransomware and phishing are especially pervasive across all sectors in Singapore, with more than one ransomware case reported every three days to the Cybersecurity Authority of Singapore. The Singapore Ministry of Health has pointed to the healthcare sector as "consistently among the top 3 most commonly targeted sectors for ransomware attacks."[19]

AFRICA

According to Check Point Research, in 2023, Africa was the global region with the highest average number of weekly cyberattacks per organization, with an average of 1,987 attacks. One in every 19 organizations in Africa experienced an attempted attack every week, an increase of 7% over 2022.[20]

The continent is challenged by the lack of digital security infrastructure. With a focus on building reliable electricity and internet to jumpstart business, cybersecurity has not been given priority. Approximately 90% of African businesses are operating without cybersecurity protocols in place, making them vulnerable to hacking, phishing and malware attacks.[21]

South Africa specifically, said by Infosecurity Magazine to be 'the world's most internet-addicted country,' is the most targeted nation in Africa for cyberattacks. In 2023, the country was also the most targeted by ransomware and business email compromise (BEC) incidents in Africa, according to internet provider Seacom. A 2023 briefing by the South African Council for Scientific and Industrial Research reported that the Rainbow Nation was the eighth most targeted country worldwide for ransomware.[22]

While South Africa's healthcare sector has not had a major attack since the 2020 attack on Life Health Care Group, the second largest private hospital, the escalation of attacks in other sectors in the country suggest that the next attack is not a question of "if" but "when."

LATIN AMERICA

19 "Singapore Cyber Landscape 2022," June 23, 2023, CSA Singapore, https://www.csa.gov.sg/Tips-Resource/publications/2023/singapore-cyber-landscape-2022

20 "A Continuing Cyber-Storm with Increasing Ransomware Threats and a Surge in Healthcare and APAC region," Check Point Research, October 25, 2023, https://blog.checkpoint.com/security/a-continuing-cyber-storm-with-increasing-ransomware-threats-and-a-surge-in-healthcare-and-apac-region/

21 Komminoth, Leo, "Africa's Cybersecurity Threat," African Business, February 23, 2023, https://african.business/2023/02/technology-information/africas-cybersecurity-threat

22 Poireault, Kevin, "Experts Urge Clearer Direction in South Africa's Cyber Strategy," Info Security Magazine, January 19, 2024

the February attack. Wired reported that RansomHub has sent the magazine several screenshots of what looked like patient records and a data-sharing contract for UnitedHealth.[17]

On April 18, 2024, Octapharma, a U.S. blood plasma provider, was subjected to a ransomware attack that closed 190 plasma centers in 35 U.S. states. The centers provide 75% of the lifesaving blood plasma supply for the U.S. and Europe. It is unclear if the company's Swiss parent, Octapharma AG, was also hit. Ransomware gang BlackSuit posted stolen data including donor information, lab data, business-sensitive information, and employee details.[18]

On April 28, 2024, Canadian pharmacy chain London Drugs discovered that it had been the victim of a cyberattack; the company has 9,000 employees and provides healthcare and pharmacy services in over 80 stores across Canada. After claiming responsibility for the attack and demanding a $25 million ransom, on

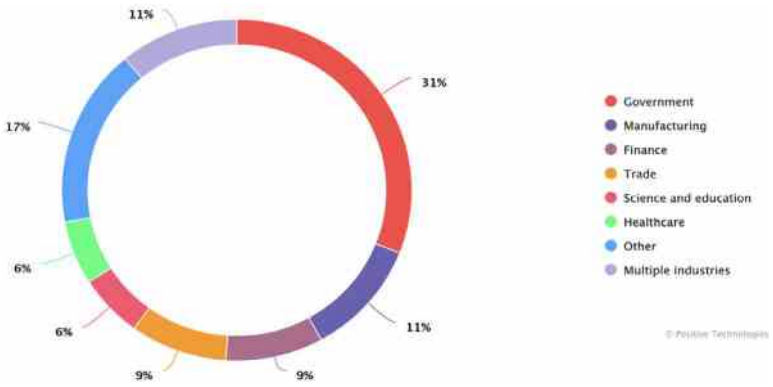
17 Geller, Eric, "Change Healthcare's New Ransomware Nightmare Gets Worse," Wired Magazine, April 16, 2024, https://www.wired.com/story/change-healthcare-ransomhub-data-sale/

18 Alder, Stephen, "OctaPharma Plasma Closes Donation Centers While It Deals with Suspected Ransomware Attack," The HIPPA Journal, April 22, 2024, https://www.hipaajournal.com/octapharma-ransomware-attack/

According to the IBM X-Force Threat Intelligence Index 2024,[23] Latin American countries account for 12% of the total number of global cyberattacks, making it the fourth most impacted region on the globe. Brazil remained the most attacked country in the region, making up 68% of all cases. Colombia accounted for 17% and Chile 8%.

The proportion of incidents which attacked the healthcare sector in the region increased from approximately 5% to 6% of total incidents over the past three years. Ransomware outpaced other attacks in the sector, accounting for 31% of the reported cases.

Phishing and use of valid accounts were each used in 22% of the reported cases. 33% of reported cases resulted in data leaks, 22% resulted in extortion.



CATEGORIES OF VICTIM ORGANIZATIONS[24]

EFFECTIVELY PROTECTING OUR HEALTHCARE INSTITUTIONS AND OUR PERSONAL INFORMATION

With the potential loss of life, and the potentially devastating effects of releasing private health information on the dark web, it is becoming increasingly vital to hospitals and other healthcare institutions to have a coordinated strategy for the protection of patients' data and delivery of health services uninterrupted by criminal actors. Investment in IT staff and well-integrated and updated systems are vital steps to meeting the most basic security requirements for healthcare.

Fortifying technical defenses, including enforcing strong

23 "IBM X-Force Threat Intelligence Index 2024," IBM, https://www.ibm.com/reports/threat-intelligence

24 "Cybersecurity Threatscape for Latin America and the Caribbean: 2022–2023," December 21, 2023, Positive Technologies, https://global.ptsecurity.com/analytics/latam-cybersecurity-threatscape-2022-2023#3

May 23 LockBit began posting 300 GB of stolen data from London Drugs including human resources medical notations, including one of a sexual assault, "harassment" negotiations with named parties, and financial files.[19]

May:

On May 13, 2024, British Columbia's First Nations Health Authority confirmed it has been the victim of a cyberattack. Officials were able to deploy countermeasures in time to prevent the attackers from encrypting its network, but the health authority said it believes "certain employee information and limited personal information of others has been impacted."[20]

On May 16, 2024, Australian federal police announced an investigation into a large-scale ransomware attack against electronic prescription provider MediSecure.[21]

19 Harnett, Cindy, 'Stolen London Drugs data posted online in ransomware attack," May 24, 2024, Times Colonist, https://www.timescolonist.com/local-news/stolen-london-drugs-data-posted-online-in-cyberattack-8811654

20 "Cybersecurity Incident," First Nations Health Authority, May 22, 2024, https://www.fnha.ca/about/news-and-events/news/cybersecurity-incident

21 Swan, David, and McSweeney, Jessica, "Police investigate large-scale healthcare data breach at MediSecure," Sydney Morning Herald, May 16, 2024, https://www.smh.com.au/technology/police-investigate-large-scale-healthcare-data-breach-20240516-p5je66.html

authentication as well as advanced threat detection systems, regularly patching software, and conducting security audits, will help to ensure malicious emails do not get through to the institution's IT infrastructure.

But in all sectors, nearly all cyberattacks begin with the cybercriminal gaining access to accounts or servers. 79 to 91% of all cyberattacks begin with a phishing or social engineering attack. The last line of defense—and perhaps the most vital line of defense—will, in the end, be the employee at the keyboard.

Security awareness training to help staff and users recognize and report potential threats such as phishing emails or suspicious activity, including regular training and drills simulating phishing and BEC attacks, not only prevent attackers from gaining access to accounts; they foster a vital culture of cybersecurity that resonates throughout the organization.

HEALTHCARE PERSONNEL PRONE TO PHISHING ATTACKS

Each year, KnowBe4 analyzes the online behavior of users to determine a baseline of how many individuals, without security awareness training, are susceptible to clicking on fraudulent links in phishing emails. For its 2024 Phishing by Industry Benchmarking report, KnowBe4 analyzed the behavior of 11 million users across various industries and sizes. The baseline statistics indicate a "Phish-prone™ Percentage" (PPP) of 34% of users; in other words, more than one out of three computer users tested were likely to click on a bad link in a phishing email.

Healthcare and pharmaceutical organizations were in the top three most susceptible industries for small and medium sized organizations, with higher PPP ratings than the baselines—34.7% and 38.8% respectively. But it was in large organizations (more than 1,000 employees) in the sector that was the most alarming; healthcare and pharmaceuticals was the most susceptible industry in the report, with a PPP rating of 51.4%. In other words, a hacker sending a phishing email to an employee of a large organization in the sector has a better than 50/50 chance of success.

The good news is that consistent and comprehensive cybersecurity awareness training works. According to the study, 90 days into an integrated approach of educational content and simulated phishing tests changed the outcomes noticeably, with the Phish-prone Percentage in healthcare and pharmaceutical organizations dropping to 21.9% in small organizations, 20.8% in medium sized organizations, and 17.7% in organizations with more than 1,000 employees.

On May 24, 2024, it was announced that the data stolen in the attack was being advertised for sale on the dark web. No figures have been released on the number of people impacted. But the company is one of two companies in Australia that allows doctors to write prescriptions to a pharmacy of a patient's choice; according to the Australian Digital Health Agency more than 122 million ePrescriptions were issued between May 2020 and March 2023.[22]

The company has requested financial assistance from the government to recover from the attack.

On May 20, 2024, Texas-based WebTPA Employer Services announced that a data breach had compromised the personal information of more than 2.4 million individuals. WebTPA is a third-party administrator specializing in health insurance and benefit plans.[23]

On May 24, 2024, Texas-based drug distributor Cencora, formerly AmerisourceBergen Corp, said that it had begun notifying affected

22 Boris, Stephanie, "MediSecure asks for government bailout after cyberhack, data advertised on dark web," ABC News Australia, May 24, 2024, https://www.abc.net.au/news/2024-05-24/medisecure-asks-for-government-bailout-after-cyberhack/103891638

23 "Notice of Data Security Incident," WebTPA, N/D, https://www.webtpa.com/notice

After one year of cybersecurity awareness training, the Phish-prone percentage dropped even more significantly; for small organizations, it dropped to 5.4%, for medium sized organizations, 4.3%, and for large organizations, 5.5%.

As the river of vital and personal information flowing through the global healthcare system continues to increase and become a growing wave, the need for a comparable strengthening of cybersecurity awareness and the creation of a security culture across the healthcare sector has accelerated and has become imperative. It can, as we are increasingly seeing, become a matter of life and death.

individuals that their personal and highly sensitive medical information was stolen from its information systems resulting from a cyberattack and data breach in February. Cencora's unit AmerisourceBergen Specialty Group (ABSG), said the information stolen was in connection with a prescription supply program offered by its now-defunct subsidiary, Medical Initiatives Inc.

On May 27, Prescription management company Sav-Rx warned the Maine Attorney General's office that the personal data of over 2.8 million people in the United States had been exposed in a data breach from a 2023 cyberattack. Also known as A&A Services, Sav-Rx is a pharmacy benefit management (PBM) company that provides prescription drug management services to employers, unions, and other organizations across the U.S.

Additional Resources

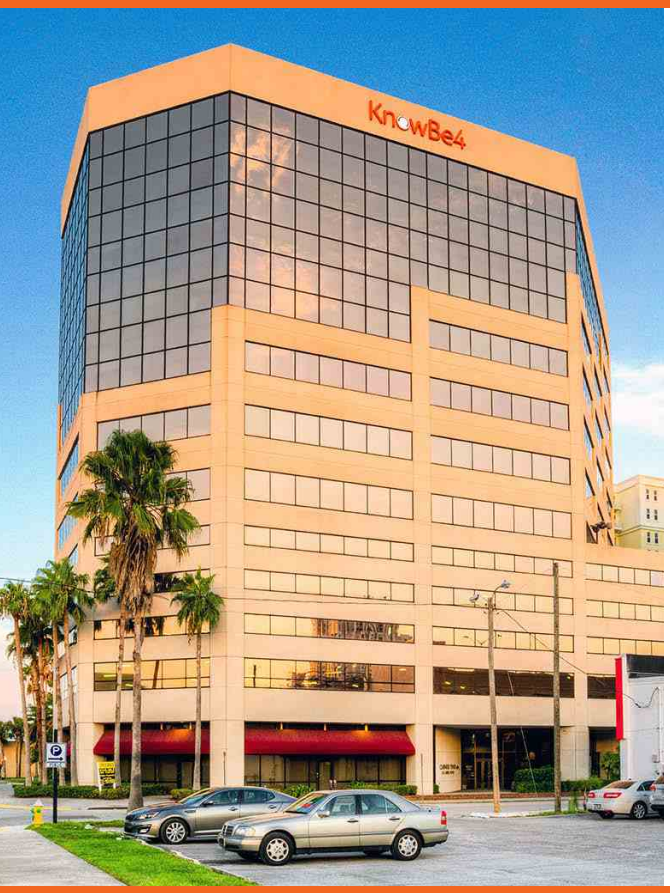
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Training Preview
See our full library of security awareness content; browse, search by title, category, language or content

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, is used by more than 65,000 organisations around the globe. Founded by IT and data security specialist Stu Sjouwerman, KnowBe4 helps organizations address the human element of security by raising awareness about ransomware, CEO fraud and other social engineering tactics through a new-school approach to awareness training on security.

The late Kevin Mitnick, who was an internationally recognized cybersecurity specialist and KnowBe4's Chief Hacking Officer, helped design the KnowBe4 training based on his well-documented social engineering tactics. Tens of thousands of organizations rely on KnowBe4 to mobilize their end users as their last line of defense and trust the KnowBe4 platform to strengthen their security culture and reduce human risk.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E06K02