Rethinking Data Security: Why Healthcare Organizations Need to See Data Differently

The list of "significant challenges faced by healthcare" varies depending on who you ask. However, among acute staffing shortages, rising costs, and pressure to implement digital health initiatives—data breaches and cybersecurity make everyone's list. Almost every healthcare organization has experienced a data incident or breach, with many having incurred multiple breaches.

Traditionally, "healthcare data" has been assumed to be patient data, such as Electronic Health Records (EHR) and insurance data. But patient data is only a fraction of the data essential to keeping the lights on in a healthcare organization. In reality, **everything** is data—information in data repositories, all applications, data flowing into and across networks, operating system software running on every digital device, collaboration apps, critical infrastructure controls—down to voice communications, employee badges and cafeteria point of sale systems. In today's threat landscape, **it's all at risk** and cyber attackers can use any of it to achieve their goals. Healthcare organizations need to reframe their perspective on what "the data" **really** is, how it's at risk, and why the ability to surveil their data is critical to their organizations and patient care.

Industry	Breaches
Finance	690
Professional	681
Unknown	651
Healthcare	571
Public administration	537

Figure 1. Reported breaches ranked by industry segment, 2022

How Many Breaches and What Do They Cost?

Data security events are classified as "incidents" or "breaches." An incident is an event that compromises the integrity, confidentiality, or availability of an information asset. A breach is an incident that results in the confirmed disclosure—not just potential exposure—of data to an unauthorized party[1].

Data breach reporting laws and requirements vary across industry, making it difficult to compare industries using exactly the same criteria. Industries also vary in their attack surfaces and abilities to detect incidents and prevent them from becoming breaches. In healthcare, 67% of incidents resulted in a breach. In comparison, only 27% of incidents in the finance sector resulted in a breach. That said, in the Data Breach Investigations Report (DBIR) 2022, healthcare ranked fourth in industries with confirmed data disclosures. Within healthcare, providers experienced 72% of the breaches, followed by business associates (16%) and health plans (12%).

[1] Data Breach Investigations Report 2022, Verizon

Healthcare breaches also tend to expose large numbers of records. According to Fortified Health Security's 2022 Mid-Year Horizon Report, the first half of 2022 saw 337 breaches affecting 19,992,810 records. Not counted in that total was one of the largest breaches that occurred during that time period but wasn't recognized until January 2023. Florida-based Independent Living Systems (ILS) experienced a breach that is affecting more than 4 million individuals. The stolen data "may have" included names, addresses, Social Security numbers, financial account information, medical record numbers, Medicare or Medicaid information, mental and physical treatment information, food delivery information, dates of birth, driver's license numbers, diagnosis codes, admission and discharge dates, billing information, health insurance information, and prescription information[2]. It's likely that the exact data stolen will never be known because the organization did not fingerprint or track its data.

Although healthcare ranks fourth in number of breaches, it's the undisputed cost leader—and has been for 12 consecutive years. In 2022, the average cost of a healthcare breach set a record high of $10.10 million[3]. The industry with the second-highest average cost is the financial industry, and it wasn't even close at $5.97 million. That figure should set off alarms at the highest level of every healthcare organization.

It's difficult to assume a direct correlation between budget spend on cybersecurity and cost of a breach, but it's interesting that healthcare also has a lower-than-average investment in security. On average, by 2022 companies worldwide allocated approximately 12.7% of their IT budgets to IT security[4]. Other reports estimate an average of up to 15%. According to a report by Astra Security, only 4-7% of health systems' IT budgets are invested in cybersecurity[5].

Who Did It and Why?

Until 2022, insiders were responsible for the majority of healthcare breaches through privilege misuse and miscellaneous errors. In 2022, external actors took over that role, with responsibility for 61% of breaches. Financial gain is the motive 95% of the time. It's not surprising, given that patient data sells for upwards of $1,000 per record on the dark web[6].

Employees were responsible for 39% of breaches, mostly due to erroneous data delivery and loss. Once again, healthcare leads industry sectors, this time in the percentage of internal threat actors. Regardless of whether or not a breach was fueled by malicious motives, the data is still disclosed. Without the ability to surveil data content, who creates it, where it travels, who uses it, and how it's used, healthcare organizations will continue to disclose significant amounts of regulated data via their employees.

[2] Health IT Security, TechTarget, March 16, 2023
[3] Cost of a Data Breach Report, 2022, IBM
[4] Average share of IT budget allocated to IT security, Statista, https://www.statista.com/statistics/1319677/companies-it-budget-allocated-to-security-worldwide/
[5] Security Audit, Astra Security, April 4, 2023
[6] Tens of thousands of patient records posted to dark web, Healthcare IT News, Feb. 8, 2021

The Second-Most-Asked Question—What Did They Get?

Although the assumption is that medical or patient data is the only—or the most—stolen data, it isn't. For the past two years, personal data has held that distinction. In healthcare, personal data was stolen in 58% of breaches. Attackers exfiltrate personal data, including email addresses, to resell and/or use for perpetrating financial fraud. Personal data of employees, contractors, vendors, and partners is every bit as breach-worthy as patient data in the eyes of an attacker. Medical or patient data was stolen in 46% of breaches. As mentioned earlier, patient data is a valuable commodity for resale and underlying identity theft campaigns. According to Onclave Networks, 95% of all identity theft incidents are enabled by stolen healthcare records.

In 29% of breaches, credentials were stolen for resale and impersonating legitimate network and system users. Stolen credentials allow attackers to easily hide out in a network and conduct reconnaissance, plant malware, and subvert legitimate IT tools and software in preparing for an attack. As we'll discuss shortly, attackers are increasingly using IT data—network credentials, vulnerable browsers, legacy software, and application and device vulnerabilities—to gain easy access to networks.

How are they doing it?

Attackers continue to use "low-tech" phishing and social engineering tactics to gain access because they work. According to DBIR, 35% of ransomware incidents used email phishing and business email compromise to gain access and prepare the attack. In 40% of ransomware incidents, attackers leveraged vulnerabilities in desktop sharing software to compromise the network. Once inside, they install malware or command-and-control (C2) software to begin exfiltrating data and setting the stage for the ransom demand. Increasingly, adversaries are choosing to simply extort ransom payments instead of encrypt the data. They already have high-value personal, patient, and credential data in hand. There's no need to mess around with data encryption and decryption (maybe) if the ransom is paid, which increases their exposure to being caught. They can simply sell data on the dark web, expose it on the public internet, or destroy it.

Email environments and outward-facing servers are the low-hanging fruit, but attackers are significantly upping their game and skills. Tactics that used to be limited to highly sophisticated nation-state bad actors are gaining popularity. In 2022, cloud exploitation cases grew by 95%, and cases involving cloud-conscious threat actors nearly tripled from 2021. Adversaries were also seen using tactics designed to modify authentication processes and target identities[7].

Supply-chain and third-party software vulnerabilities are emerging as major threat vectors. Threat actors are increasingly weaponizing popular, legitimate IT management tools, such as endpoint management, remote desktop sharing applications, and network asset management systems for malicious purposes. Many of these tools are open source and easy to obtain with the added benefit of actors being able to use them while evading detection.

[7] 2023 Global Threat Report, Crowdstrike

Legacy software and devices offer more easy avenues for attack. Just recently, an employee of 3CX, makers of a popular voice-over-IP system, used his credentials to download and install a financial trading application on his computer. The downloaded trading application had been retired by its maker in 2020, but was still widely available. In early 2022, it was compromised and infected with a back-door malware. Once installed on the employee's computer, attackers were able to access 3CX's software build environment and replace a Dynamic Link Library (DLL) file in the 3CX app with a trojanized version. Now when the 3CX app is loaded on any computer, it functions as full-blown malware that beacons to remote servers and is capable of running second stage malware. The impact is global—the 3CX desktop app is used by hundreds of large businesses, governments, and service providers. It's safe to say that few, if any, of these 3CX customers even thought to scrutinize their updated software down to the binary level.

The bottom line is that most organizations simply trust the software provided by vendors. In today's threat landscape, every organization needs to have eyes on all of its data—especially that which comprises its IT, cloud, and security infrastructures.

What About Our Current Defenses?

Healthcare organizations have typically based their security defenses on compliance requirements. HIPAA is the most well-known regulation in healthcare, but there are many others. Compliance regulations recommend general types of controls, but none prescribe specifics as to the best way to secure an organization's network and data.

Network access controllers (NACs) are commonly used to control user and device access to networks and network segments. New Zero Trust approaches still focus on device and user authentication for access. None of these measures focus on protecting the data itself.

Data leak prevention (DLP) systems are also widespread in healthcare security infrastructures. In today's rich data environments, they are increasingly challenged. They only identify predefined data patterns, inspect only a fraction of actual organizational traffic, and only operate at the point of data leaving the network. These systems are rarely updated and easy to defeat. They're certainly not designed to cope with high volumes of modern network traffic that includes images, collaboration channel threads, email, PowerPoint presentations, video, audio streams, and internet searches.

Going one step further, not all data essential to running the clinical and administrative sides of the business is subject to compliance. Financial data, operational data, critical infrastructure, analytics, applications, IT system, policy data, and persistent data stored in systems across the organization are essential for day-to-day operations. Yet the security focus has been primarily on patient data. As attackers weaponize legitimate IT and security software, compromise cloud environments, and step up their mobile malware game, healthcare's current defenses are woefully inadequate. The proof is everywhere. None of these defenses have stopped data breaches, and they continue to increase.

Time for a Turnaround

The bottom line is that attackers continue to target healthcare data and win. Healthcare organizations are paying more than twice the cost of any other industry to simply mitigate the results of a breach—with no guarantee of recovering any lost data. At the same time, without security investments keeping pace, they're falling farther behind in the cyber attacker "arms race." They are easy targets.

Data Surveillance: Eyes on All of Your Data, Everywhere, All the Time

It doesn't have to be this way. It's time to start protecting the data itself and not just the networks, devices, and clouds containing it.

Flying Cloud Technology is the only company committed to securing what matters most—the data itself. With more than two decades of security expertise and nine data surveillance patents, we're enabling companies to look at their data analytically and forensically with the ability to control where it moves. For the first time, you can see, track, and defend your data, using those capabilities for a wide range of security and operational purposes.

Flying Cloud CrowsNest data surveillance delivers real-time visibility into data structure, content, movement, and usage at the binary level. You'll gain a data chain of custody that documents who creates data, who consumes it, where it moves, and how it changes.

See the Data—Any Data. All Data.

CrowsNest data surveillance delivers visibility into any and all data, both structured and unstructured. This includes data like diagnostic imaging, video, email, PowerPoint presentations, collaboration threads, spreadsheets, audio streams, asset inventories, application code, device configurations, and internet searches. CrowsNest AI technology can even identify screen shots or pictures shot with a phone if that binary data comes across the network.

Data surveillance begins by interfacing with any data repository through a simple API. Next, CrowsNest fingerprints the data, cataloging all identified data without touching or modifying the data in any way. Working at the binary level, CrowsNest identifies where the data originates, as well as its purpose, level of sensitivity, structure, movement, and relationship to other data and users.

Track the Data

Once data is fingerprinted, CrowsNest follows the data everywhere it goes on the network. Patented machine learning and automation quickly establish a baseline of normal and acceptable data patterns. When fingerprinted data behaves out of character with the rolling baseline, CrowsNest alerts you to a security event.

CrowsNest can automatically classify data, eliminating manual methods of tagging data or relying on users to make decisions about where to place documents. Create your own categories—file type, keyword, devices, users, time sensitivity, or others—and determine where you want content to reside. You can "data fence" content, restricting its movement with granular specificity based on the content, IP address, or other parameters. This means you can create policy for data that restricts which content can go where—down to physical spaces within buildings if needed.

CrowsNest also recognizes non-fingerprinted data on the network that fits your policy or classification requirements. This means you can be alerted to sensitive data that is moving or being used in violation of security or compliance requirements, and stop it before it becomes a potential breach.

Defend the Data

CrowsNest defends your data by identifying anomalous data behavior in real time. Data policies in CrowsNest can include tunable data exfiltration parameters. Any attempt to exfiltrate data—whether on the network to an external location or any movement of data attempting to leave a specific area—triggers an alert.

CrowsNest also identifies and isolates cyber threat activity occurring in data. It automatically detects data behaviors that are characteristic of ransomware, botnets, malware, Bitcoin, back doors, and command-and-control software. It will alert your team, as well as trigger action by other security solutions, if desired.

Your team receives contextual analysis, including reconstructed events, extracted payloads, and play-by-play analysis of the activity. Teams will know exactly what happened, where, and by whom—gaining a data chain of custody to support response and remediation. You can also have CrowsNest deliver full digital forensics data to a SIEM.

Enable and Protect Your Organization, Employees, and Patients

The bottom line for your organization usually revolves around that—the bottom line. Data surveillance is a foundational capability for securing healthcare organizations while at the same time providing data accountability and governance. It's the only way to protect the data itself at the binary level while integrating seamlessly with your existing security controls.

Protect Data Everywhere

When you can visibly see the data you have, you can begin to protect it more effectively. Prioritize the data most at risk and align defenses accordingly. Start with patient data, and easily expand visibility across critical IT, clinical, and administrative environments based on the data of most value to your specific organization. Gain comprehensive data accountability—otherwise, you're simply guessing.

Reduce Complexity

Augment existing security solutions with data surveillance capabilities or replace them where appropriate, and gain better protection with much more flexibility in the types of data you can track and defend.

Reduce Costs

Visibility enables a team to do far more with the resources they have. Eliminate aging DLP systems by implementing their rulesets into CrowsNest. Customers not only meet their compliance requirements, they gain a ledgerized view of their data. Several have achieved savings up to $250,000/year in maintenance costs associated with their previous DLP systems.

Fit Your Infrastructure Today and Tomorrow

Integrate CrowsNest easily into existing security infrastructure—with NACs, firewalls, SIEMs, DLP solutions, IoT solutions, and cloud security—without impact on users or systems. In the cloud, on premises, or in hybrid environments, CrowsNest can be implemented per dataset, per site, or enterprise-wide to automatically surveil and defend data at any level and at any scale.

Don't Be a Statistic

See data differently and transform security effectiveness. Protect your data from current and emerging threats with the ability to see, track, and defend it across your organization. Ask for a discovery engagement with CrowsNest today.

For more information, request a meeting.
Or visit us at www.flyingcloudtech.com.

About Flying Cloud

Flying Cloud secures the one thing that matters most—data. We enable organizations to see their data as it is created, moves, and is consumed across the network. Founded in 2014, Flying Cloud holds nine data surveillance patents. Our CrowsNest data surveillance solution gives customers the first-time ability to look at their data analytically, forensically, as well as control where it goes. Flying Cloud is privately held.