Critical Insight

Healthcare Breach Report

July-Dec 2021

Security Research and
Data Analysis

Table of Contents

Overview

As we enter the second year of the pandemic, healthcare systems are under unprecedented and unrelenting stress. Frontline healthcare workers are understaffed and overworked. Hospitals are so overcrowded that they have been forced to postpone routine medical procedures until the latest surge of COVID-19 cases subsides.

Similarly, IT departments at healthcare organizations are facing critical skills and staffing shortages as they battle the latest cyberattack variants. They're stretched so thin dealing with pandemic-related crises that routine security measures may fall by the wayside, breaches may go undetected for months, and efforts to validate the security measures undertaken by affiliates and third parties may fall short.

Critical Insight's latest analysis of breaches reported to the U.S. Department of Health and Human Services by healthcare organizations shows that the total number of breaches and the total number of records of protected health information (PHI) that were exposed hit all-time highs in 2021.

The silver lining is that the number of reported breaches and the number of individuals affected declined slightly over the second half of 2021, compared with the first half of the year. It's too early to tell if that modest improvement represents the beginning of a longer trend in the right direction.

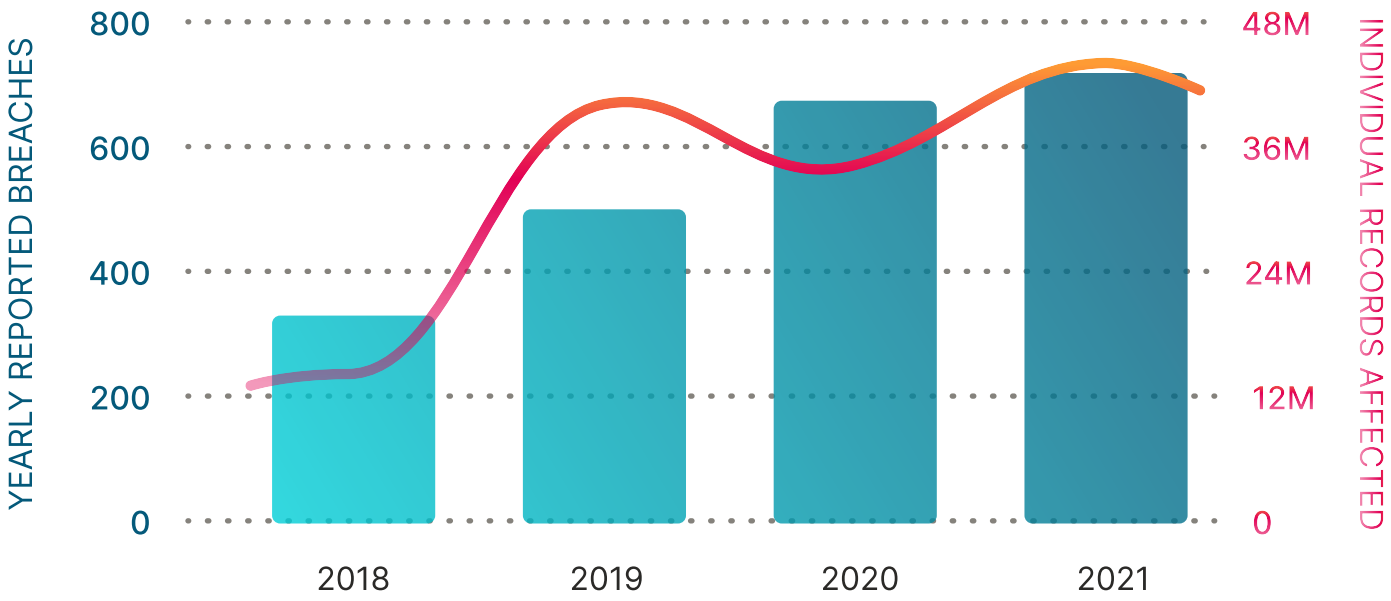
The results could indicate that security teams have done a good job shoring up their defenses (either internally or through partnerships with managed security providers) in response to the surge in attacks that occurred in 2020, when cyber-criminals ramped up their efforts to take advantage of vulnerabilities that were exposed during the early, chaotic days of the pandemic.

However, this is no time for security teams at healthcare organizations to let their guard down. Attackers are aiming at bigger targets. Exploits, particularly ransomware, are becoming more sophisticated. And cybercriminals are expanding their activities to take advantage of security vulnerabilities across the healthcare supply chain, from business partners to health plans to outpatient facilities.

Healthcare breaches and the individuals affected by them are on the rise year over year, with an

84% increase in the total number of breaches between 2018 and 2021. The total number of individuals affected has tripled over the same period, from 14 million in 2018 to 45 million in 2021.

Total Breaches and Individuals Affected Over Time



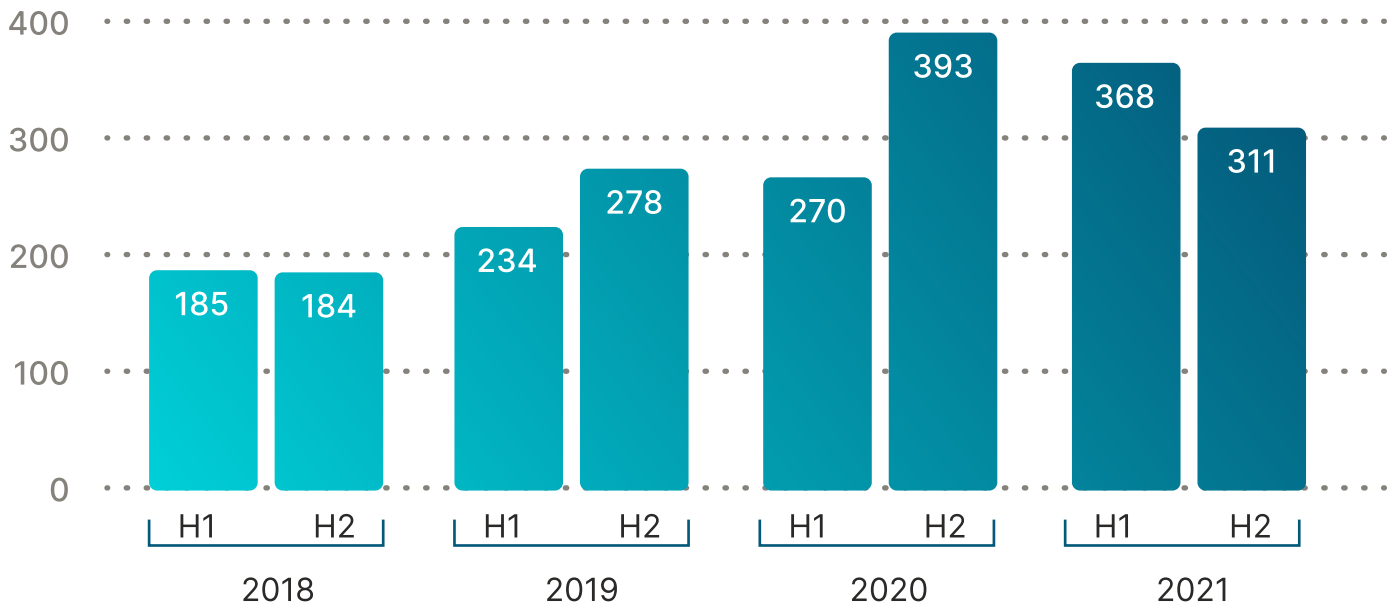
	2018	2019	2020	2021
Individuals	14.14M	42.37M	34.03M	44.91M
Breaches	369	512	663	679

Key Findings

- The total number of individuals affected increased 32% over 2020, meaning that more records are exposed per breach each year.
- The total number of breaches only rose 2.4% from 2020 but still hit historic highs.

While breaches have increased year over year, when we look at half year totals we see that we may have begun a downward trend after a spike in the second half of 2020. This spike may have been due to healthcare organizations being too busy to report during the first half of 2020, when the pandemic first hit, or may have been due to dwell time, when the attackers were inside the systems unnoticed. The number of individuals affected follows the same trend along half years, declining from a spike of 26 million in the second half of 2020, to 24 million in the first half of 2021, to around 21 million in the second half of 2021.

Total Breaches Reported by Half Year



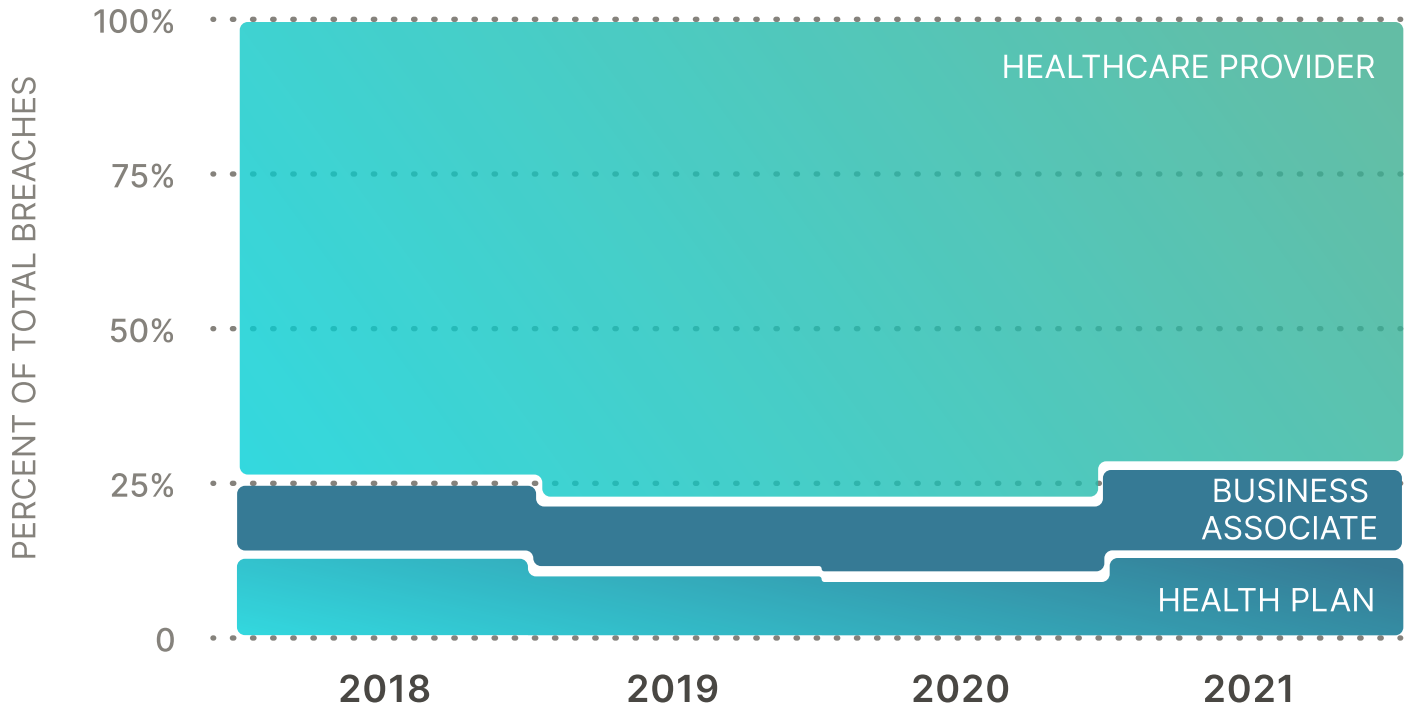
Key Finding

- Breaches have declined over the past two reporting periods, but are still higher than pre-pandemic levels.

Who is Getting Breached?

As we look at the increase in healthcare breaches reported over recent years, it is important to consider their targets, and how breaches have changed over time in certain healthcare subsegments. Healthcare providers continue to be the dominant entity who is breached, but attacks on business associates expose more records per breach than other entities.

Breaches by Entity

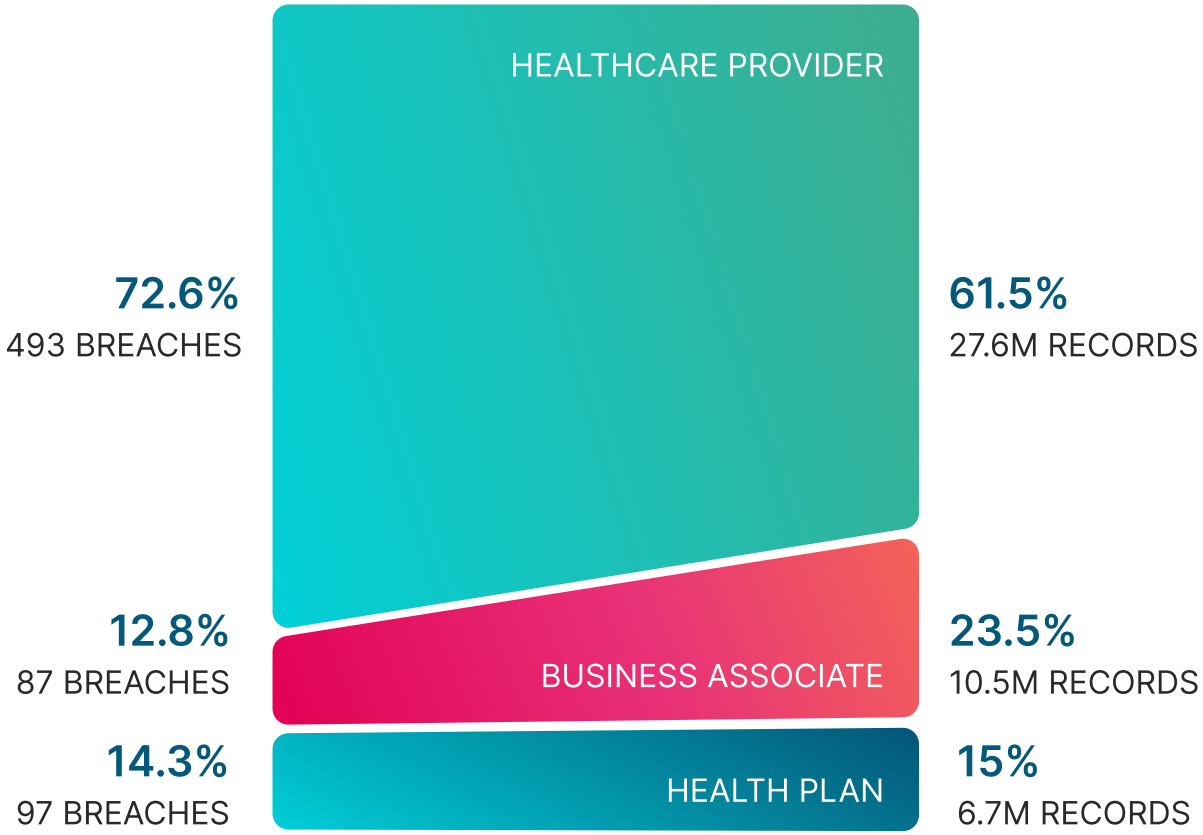


	2018	2019	2020	2021
Provider	273	397	515	493
Business Associate	42	54	74	87
Health Plan	53	59	72	97
Other	1	2	2	2

Key Findings

- Healthcare providers still make up the majority of successful attacks.
- Attacks against health plans jumped nearly 35% in 2021.
- Attacks against business associates, or third party vendors, increased nearly 18% from 2020.

2021 Breaches Involving Business Associates



A small percentage of other healthcare providers accounted for 2 breaches (0.3%) and 2,462 records.

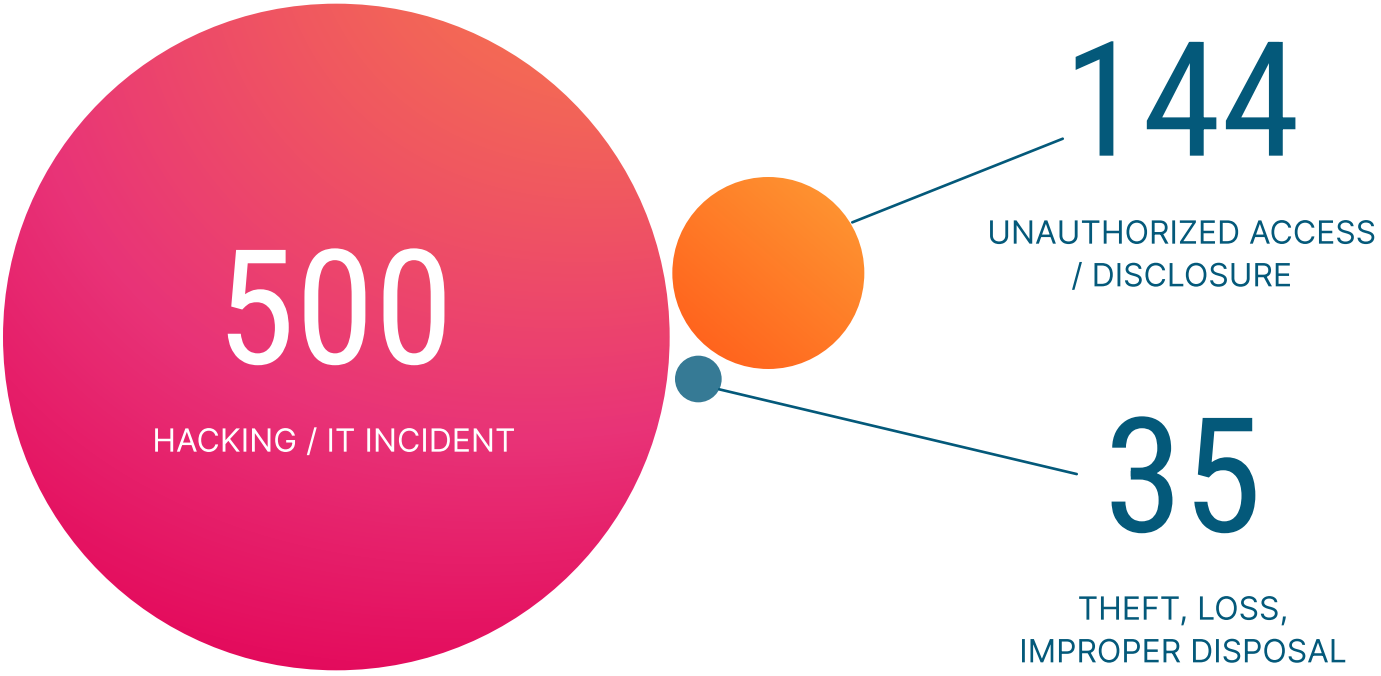
Key Findings

- Business associate breaches have risen in frequency, and in 2021 involved far more records per breach than other healthcare entity type.
- Business associate-related breaches accounted for nearly 13% of total breaches, but almost one quarter of the total individual records.

What Are the Most Common Breach Causes?

Hacking/IT incidents are by far the most common breach type. They rose 9.9% between 2020 and 2021, from 455 to 500 reported, which fortunately is a smaller increase than in previous years. Unauthorized access rose slightly in 2021, but theft, loss, and improper disposal stayed relatively low. These breach types can be prevented by security training, and thus may indicate that entities are taking steps to protect their data.

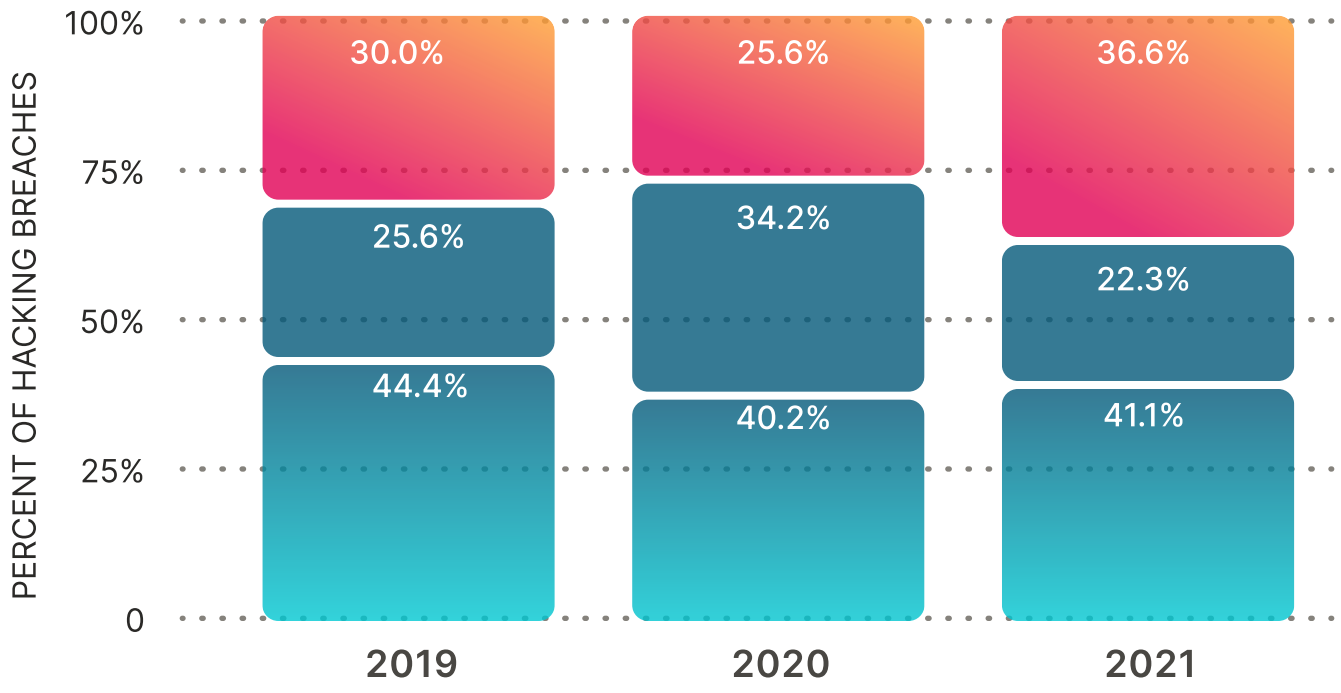
2021 Total Breaches by Type



Key Finding

- Hacking/IT incidents were responsible for the majority of individual records that were affected by breaches which could indicate those records were sold on the Dark Web.

Hacking Breaches by Healthcare Provider Microsegments



	2019	2020	2021
Clinic / Outpatient	75	93	131
Hospital Systems	64	124	80
Other	111	146	147

Key Finding

- Hacking/IT incidents on Healthcare providers are the most common, both by breach type and entity.
- Outpatient/specialty clinics have seen a 41% increase in hacking/IT incidents in the last year.

How Are Healthcare Providers Targeted?

"Since 2019, the healthcare sector has seen a shift from breaches caused by internal actors (either malicious or by mistake) to primarily external actors. This is good news, as no industry wants their employees to be their primary threat actor," according to the 2021 Verizon Data Breach Investigations Report.

"Financially motivated organized criminal groups continue to target this sector, with the deployment of ransomware being a favored tactic," says the report, which broke down the motives behind attacks as 91% financial, 5% fun, 4% espionage and 1% grudge.

Michael Hamilton, CISO at Critical Insight agrees that "we will see continuing ransomware attacks." But he also predicts that "efforts by the federal government to stop ransomware payment mechanisms, identify and apprehend gang members, and disrupt their infrastructure will show success."

In the meantime, healthcare companies need to pay attention to all the other tricky ways that attackers are getting their hands on PHI. Here are some recent examples that show how difficult it is to protect against advanced attack techniques.

Accellion is a technology provider that sells file transfer appliances (FTA) that help companies move large email attachments. The ransomware group called Clop took advantage of a vulnerability in the Accellion gear to launch ransomware attacks against hundreds of companies, primarily targeting the healthcare sector. An estimated 3.5 million healthcare records were breached from dozens of companies impacted by the attack.

20/20 Eye Care Network reported that 3.3 million patients had their health information stolen after an Amazon Web Services cloud storage bucket that was not properly configured and protected.

CaptureRx provides third-party administrative services to the healthcare industry. CaptureRx was hit with a ransomware attack that exposed the records of 2.42 million patients at multiple healthcare organizations including a hospital in New York, a community health center in Texas and a pharmacy chain in the Midwest.

At St. Joseph's/Cander Health System in Georgia, a ransomware attack stole data associated with 1.4M patients. An investigation revealed that

the hackers gained access to the system more than six months before deploying the ransomware.

These examples highlight the challenges that healthcare organizations face. Even if the organization is able to improve its own internal processes, protect its remote workers, keep patches up to date, secure mobile devices and make sure cloud-based systems are properly configured, that's not enough.

What You Can Do

Healthcare organizations must get their arms around third-party risk through a comprehensive risk management program. To begin with, organizations should classify their business associates by level of risk based on the type of data that third parties are able to access.

Organizations need to establish procedures and processes associated with vetting third parties before granting them access to data.

And, companies should be sure to emphasize security in any business agreement with third parties. Find out what types of security policies they have in place for data protection. Have they recently passed a security audit? What are their procedures for reporting breaches? Is it possible to contractually require incident reporting to business associates?

Additionally, healthcare organizations should be constantly on guard for intrusions. Security teams may feel that they are overmatched, spending most of their time putting out fires, but Critical Insight can provide important services, such as managed intrusion detection and response.

With this type of capability, instead of an attacker slowly bleeding data out of your organization over a period of months, the attack is quickly detected, and the bleeding is stopped. The next step is figuring

out what went wrong and fixing whatever vulnerability existed.

Of course, in security and in healthcare, prevention is always preferable to a cure. Critical Insight offers penetration testing, incident readiness planning, vulnerability management and cybersecurity risk assessments so that healthcare organizations can stay one step ahead of the bad guys, and demonstrate compliance with regulatory requirements and standards of practice.

Contributors

John Delano

John has three decades of IT experience, much of it in Healthcare as a CIO. He's currently the Vice President of Ministry & Support Services for CHRISTUS Health.

Michael Hamilton

Michael has more than 30 years' experience in Information Security, working in every imaginable role. He's a co-founder of Critical Insight, its spokesperson, and CISO.

Trisha Lowe

Trisha has built a career around analyzing data to improve businesses and the resulting customer experience. She is currently the Chief Experience Officer for Critical Insight, previously running Business Analytics.