Critical Insight

HEALTHCARE BREACH REPORT

Security Research and Data Analysis

Jan - Jun 2023

TABLE OF CONTENTS

REPORT OVERVIEW

In the first half of 2023, there was a notable decrease in the overall number of data breaches impacting healthcare organizations. However, this encouraging trend was overshadowed by a few major breaches, causing a significant increase in the number of individuals affected, reaching record levels.

Dental benefits administrator, Managed Care of North America, fell victim to a severe cyber-attack that compromised 8.9 million individual records. Similarly, PharMerica, a pharmacy services provider, was targeted by ransomware, resulting in the exposure of 5.8 million records. Additionally, numerous other breaches occurred, each impacting ~3 million of individuals.

NEW STRATEGIES IN CYBER ATTACKS: TARGETING THE WEAKEST LINKS IN THE SUPPLY CHAIN

Cyber attackers are now targeting vulnerable points in the supply chain, specifically the business associates or third-party companies that offer services to healthcare organizations.

One example is NationsBenefits Holdings, a provider of supplementary benefits solutions to managed care providers, which disclosed that a breach originating from its third-party cybersecurity services provider impacted 3 million individuals.

The US Department of Health and Human Services (HHS) collects and analyzes the breach information that healthcare organizations are obligated to report that compromise over 500 individual records within 60 days of detection.

Frontline healthcare organizations must be constantly vigilant about their security vulnerabilities. It is crucial for them to also ensure that all the companies they work with in their supply chain uphold the highest level of security readiness.

KEY TAKEAWAYS

Critical Insight's analysis of breach data supplied to the US Department of Health and Human Services (HHS) reveals the following key findings for the first six months of 2023.

1. **Evolved Attacker Tactics:** There were fewer, but bigger breaches, which reflects consolidation within the industry and the evolving tactics of attackers.

2. **Breach Numbers Decrease:** The total number of breaches has decreased by 15% as compared to the second half of 2022. This year is on track to record the fewest breaches since 2019.

3. **Increase in Exposed Records:** The number of individual records compromised in data breaches surged by 31% in the first half of 2023, compared to the second half of 2022.

4. **Hacking and Extortion Strategies:** The majority (73%) of all breaches in the first half of 2023 are attributed to hackers. Attackers seem to be changing strategies, some employing “double extortion” in which they charge victims once for decryption and once for the stolen data. Others are shifting away from encryption to solely “single-extortion” in which they demand payment for stolen data. Without the revenue from encryption, some criminals have also reached out directly to patients, demanding money.

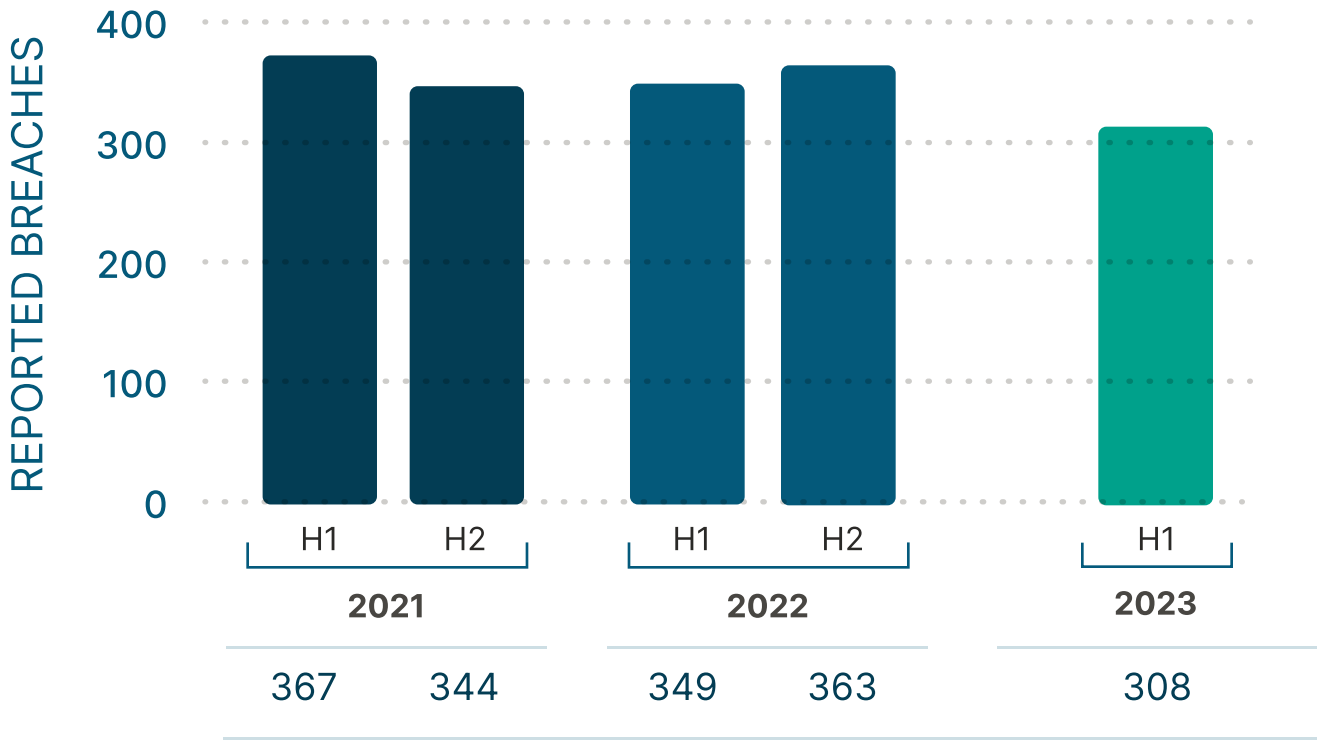
THE HEALTHCARE BREACH LANDSCAPE

The number of reported breaches in the first half of 2023 decreased by 15% compared to the second half of 2022. This is a positive trend considering the steady increase in attacks over the past few years.

HISTORICAL BREACHES

- **367 in the first half of 2021**
- **344 in the second half of 2021**
- **349 in the first half of 2022**
- **363 in the second half of 2022**

In 2019, the total annual breaches were 506, and in 2020, it rose to 661. However, the reduced number of breaches in the first half of this year suggests that the overall number may be lower for the entire year.



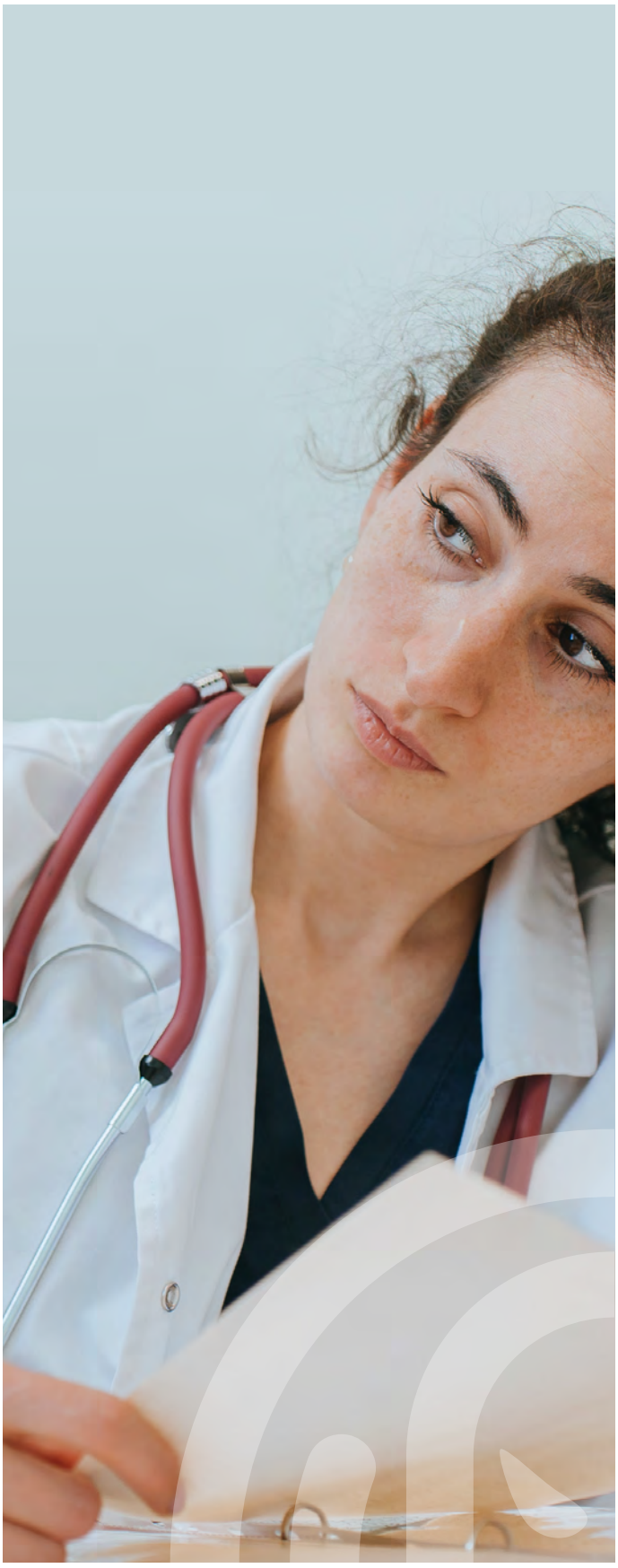
LANDMARK BREACHES

While the total number of breaches declined over the latest reporting period, the number of individuals affected jumped sharply, from 31 million in the second half of 2022 to 40 million, which is the highest number on record for a six-month period.

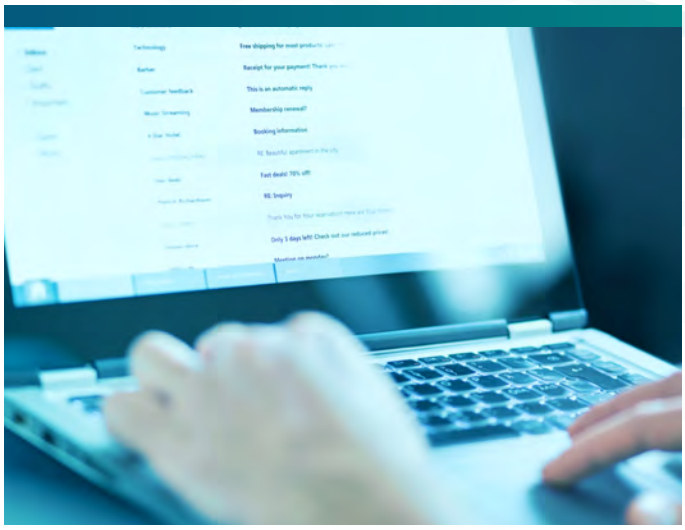
31 million in the second half of 2022 to 40 million, which is the highest number on record for a six-month period.

The Managed Care of North America and PharMerica breaches were the third and fourth largest ever reported.

The average number of individuals affected per breach also hit an all-time high of 131,000, which reflects the lower number of breaches and the impact of the large breaches on the overall average.



We're on pace to shatter the record for individuals affected by breaches. The high-water mark was 58 million in 2021, and we're already at 40 million, or 74% of the total number of individuals affected in all of 2022.



WHAT ARE THE CAUSES OF DATA BREACHES?

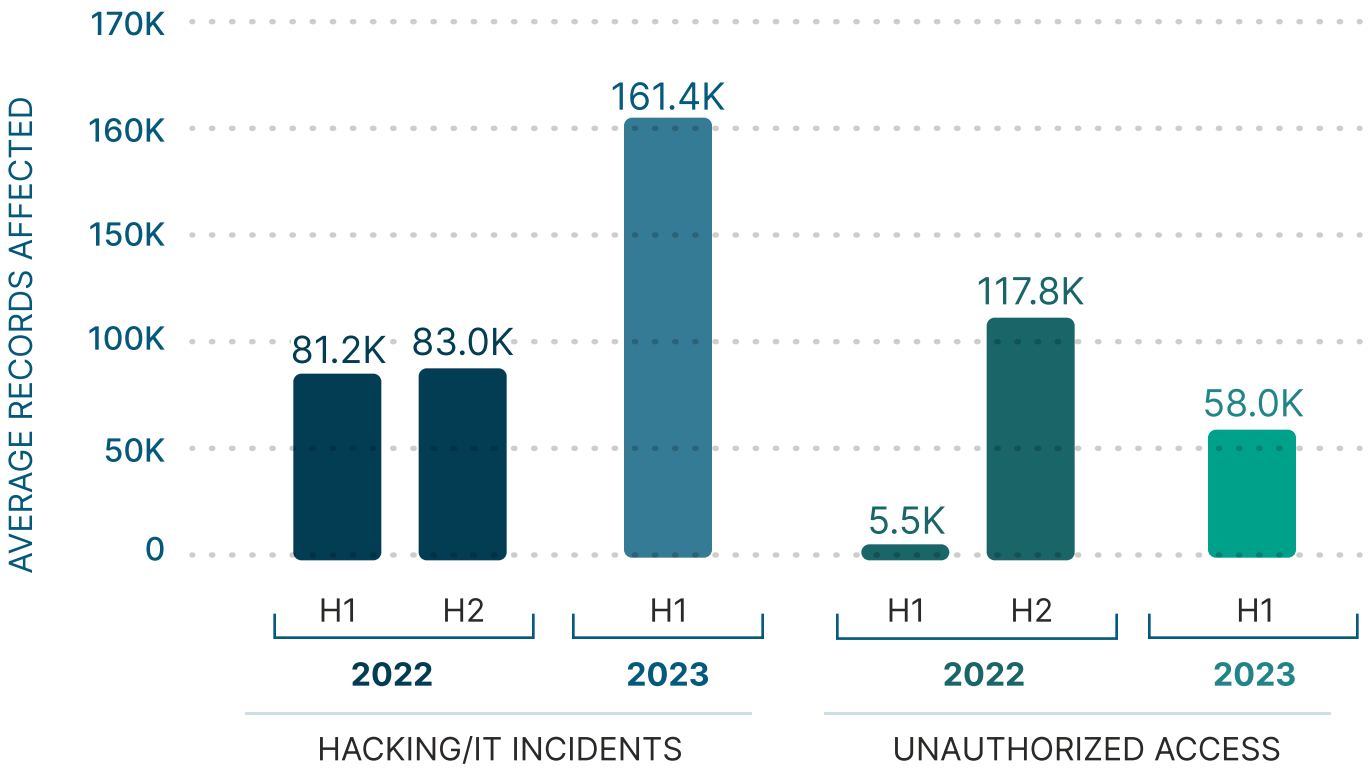
Causes of data breaches can be attributed to various factors. According to the reporting process, the five possible types of breaches include hacking/IT incidents, unauthorized access/disclosure, theft, loss, and improper disposal.

Among these, hacking/IT incidents were found to be the primary cause, accounting for a significant 73% of breaches in the first half of 2023.

Unauthorized access/disclosure was the second-most prevalent type, with a notable increase from 15% in 2022 to 23%.

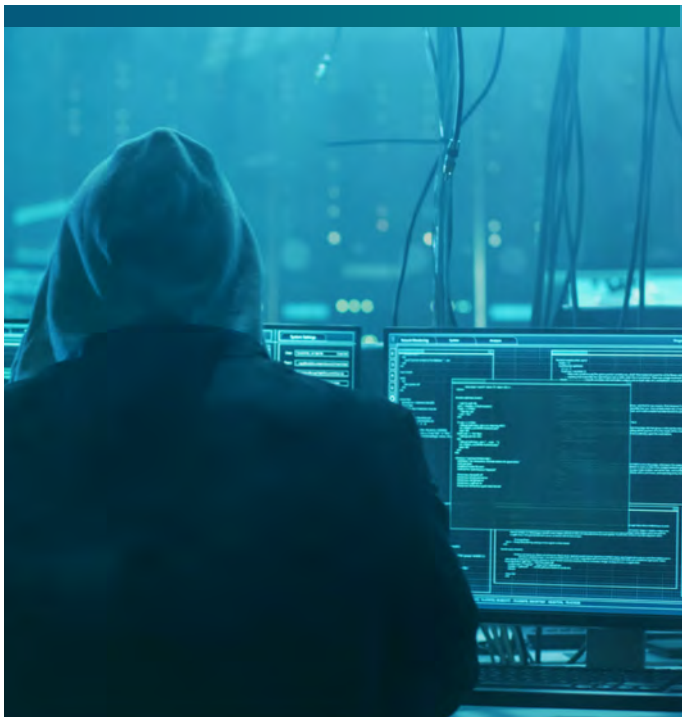
Theft, lost records, and improper disposal were relatively insignificant contributors to data breaches.

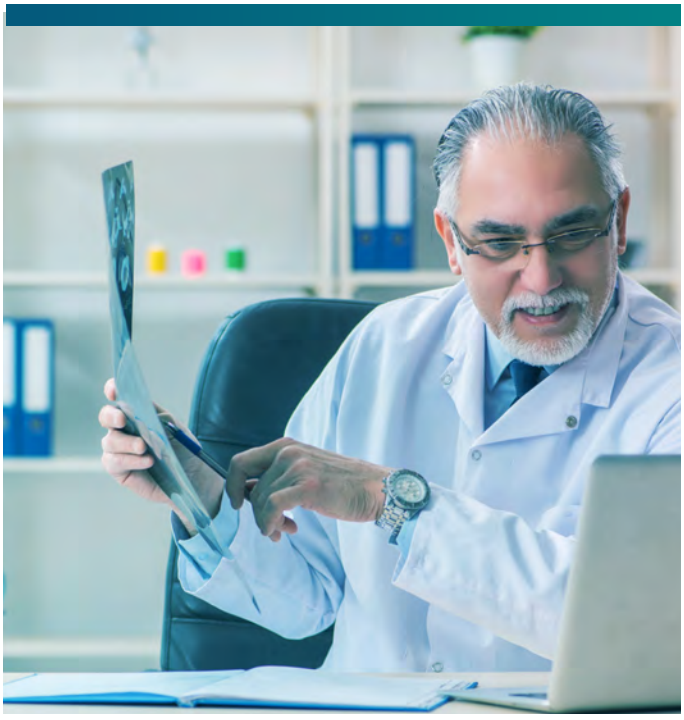
AVERAGE RECORDS AFFECTED BY BREACH TYPE IN 2023



BREACH TYPES

A total of 308 reported breaches have been analyzed, revealing a steady pattern in the breakdown of breach types. Hacking accounts were the majority with 225 incidents, followed by unauthorized access with 70 incidents. Additionally, theft was blamed for 8 breaches and 5 on improper disposal. This data aligns with trends observed since 2019.



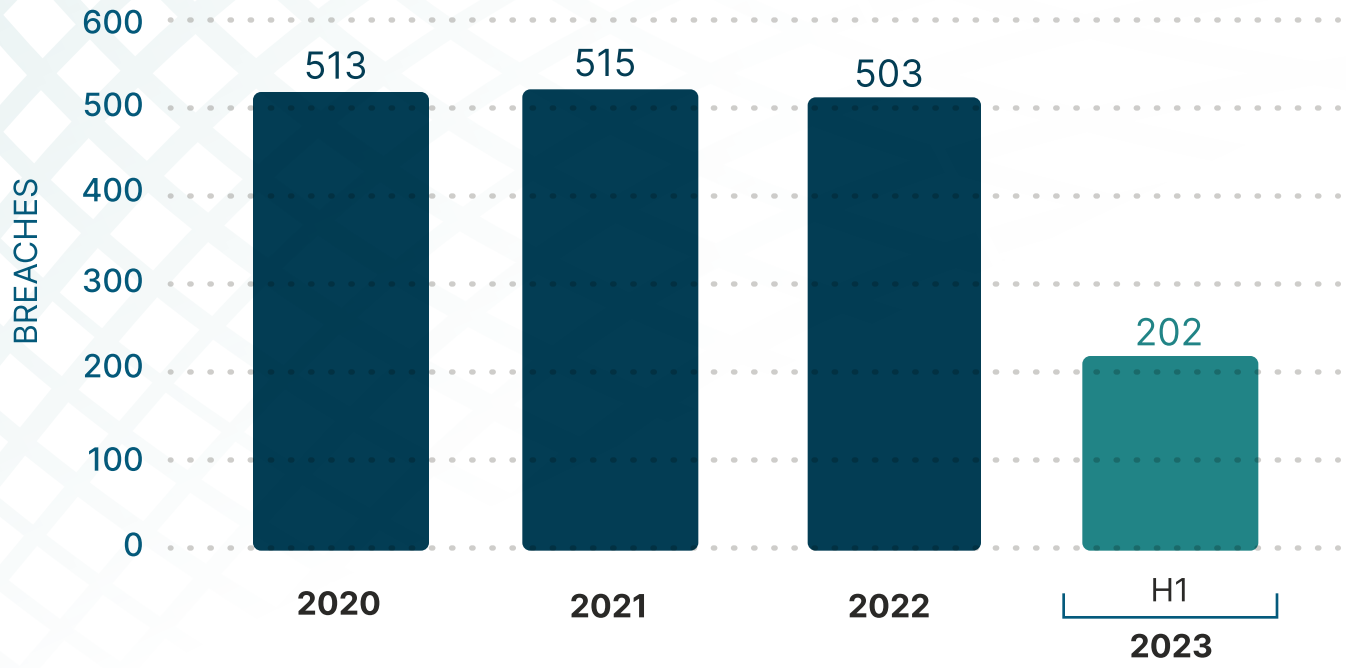


BREACH STATISTICS

In the first half of 2023, the healthcare industry experienced a staggering 40 million records compromised in data breaches. 90% of these breaches were the result of hacking incidents, while unauthorized access accounted for most of the remaining percentage.

NUMBER OF OVERALL BREACHES

Healthcare providers remain a prime target for hackers, despite their widespread focus on every link in the supply chain. In fact, 65% of healthcare breaches in the first half of 2023 specifically targeted healthcare providers. However, the good news is that the data from this period suggests that **we are on track to experience fewer provider breaches compared to the previous three years.**



INCREASE IN THIRD-PARTY ASSOCIATE BREACHES

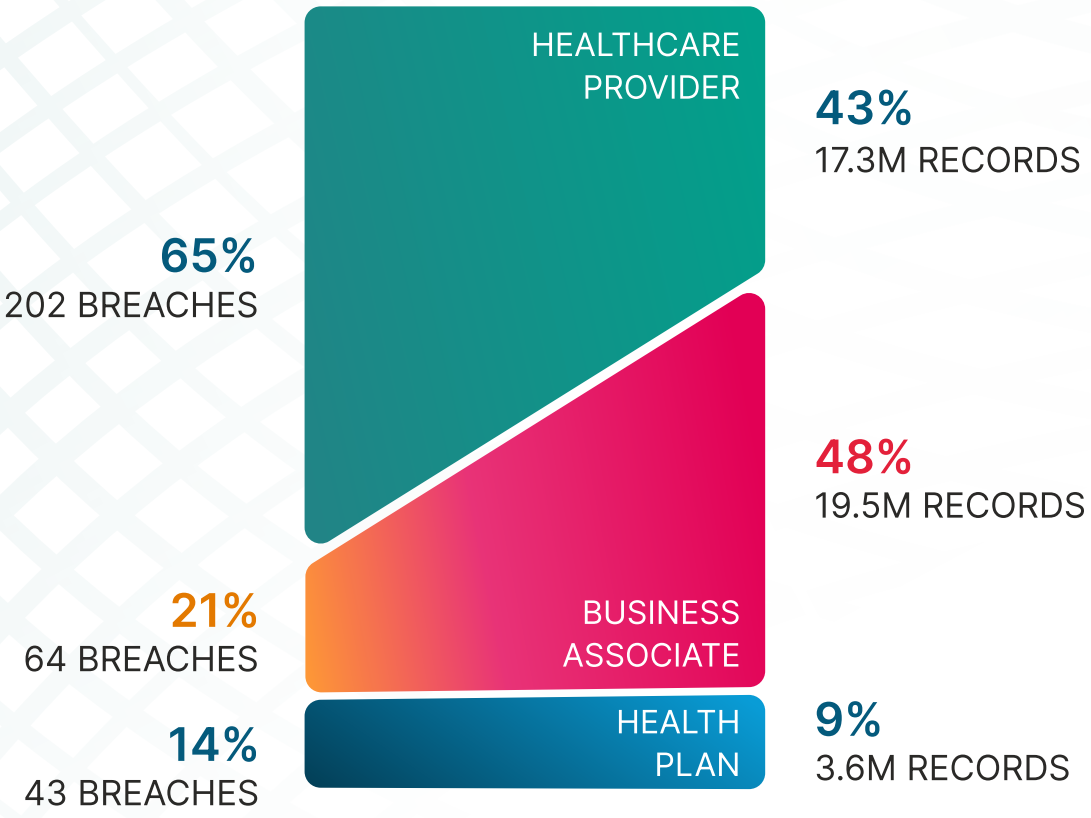
In recent years, hackers have intensified their attacks on third-party business associates, raising alarms among healthcare providers. While the percentage of provider breaches has shown a slight decline, from 81% in the second half of 2019 to the current 65%, a concerning trend has emerged.

The percentage of breaches associated with business associates has steadily risen, jumping from 10% in the first half of 2019 to 21% in the first half of 2023. This escalating threat places healthcare organizations at increased risk, highlighting the urgent need for enhanced cybersecurity measures.

In the first half of 2023, breaches involving business associates affected 304,191 individuals on average per breach. This is significantly higher than the average number of individuals affected per breach in healthcare provider breaches (85,680) and health plan related breaches (84,240).

INDIVIDUALS AFFECTED BY ENTITY TYPE

While healthcare providers have three times as many breaches as business associates, the actual number of individual records affected tells a different story.



Out of the 40 million exposed records, 48% (19.5 million) were linked to business associates, while 43% (17.3 million) were associated with healthcare providers.

The presence of a business associate in data breaches saw a dip in the second half of 2021 but has since climbed back up to 33% in the latest reporting period. Although this percentage is lower than the levels seen in 2022, it remains a significant concern.

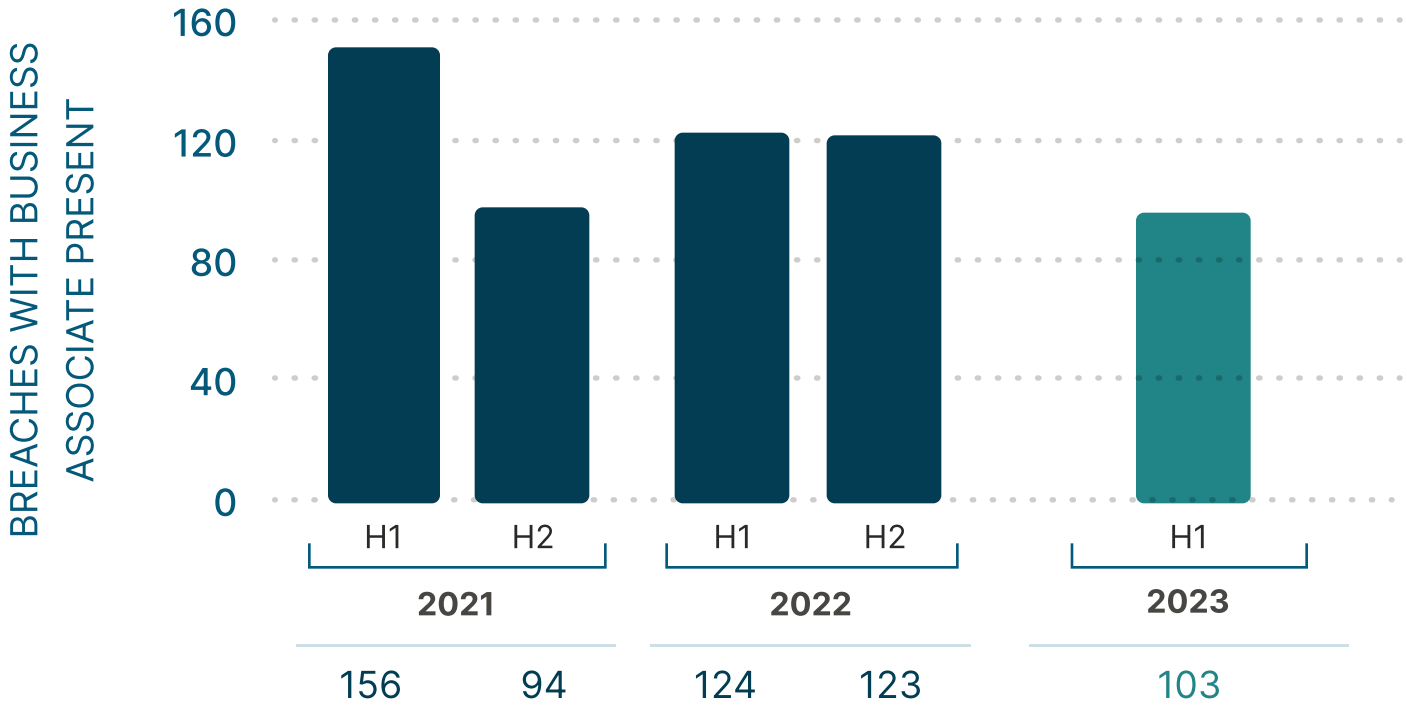
TOTAL BREACHES: BUSINESS ASSOCIATE PRESENT

Since many business associate breaches affect a high number of individuals, the percentage of affected individuals – with a business associate present – varies from reporting period to reporting period.

In the first half of 2023, 50% of individuals impacted by a breach had a business associate present. This represents an upward and consistent trend as compared to previous years.

BREACHES WITH BUSINESS ASSOCIATE PRESENT

- **27% in the second half of 2021**
- **36% in the first half of 2022**
- **34% in the second half of 2022**
- **33% in the first half of 2023**



Critical Insight

https://criticalinsight.com

Healthcare providers continue to be the covered entity most breached by hacking/IT incidents at 62%. The percentage of reported incidents has improved compared to previous periods, with a decrease from 80% in 2020 to 71% in 2021 and 73% in 2022. However, the percentage of hacking/IT incidents involving business associates has consistently increased from 12% in 2020 to 13% in 2021, 17% in 2022, and currently stands at 25%.

DECREASE IN BREACHES AND HACKING INCIDENTS

During the first half of 2023, the number of breaches witnessed a significant decline. In particular, hacking-related breaches dropped by 20% compared to the second half of 2022.

Notably, healthcare providers, who were previously responsible for 84% of these breaches in the second half of 2020, now only account for 62% - the lowest percentage since reporting began 2019.

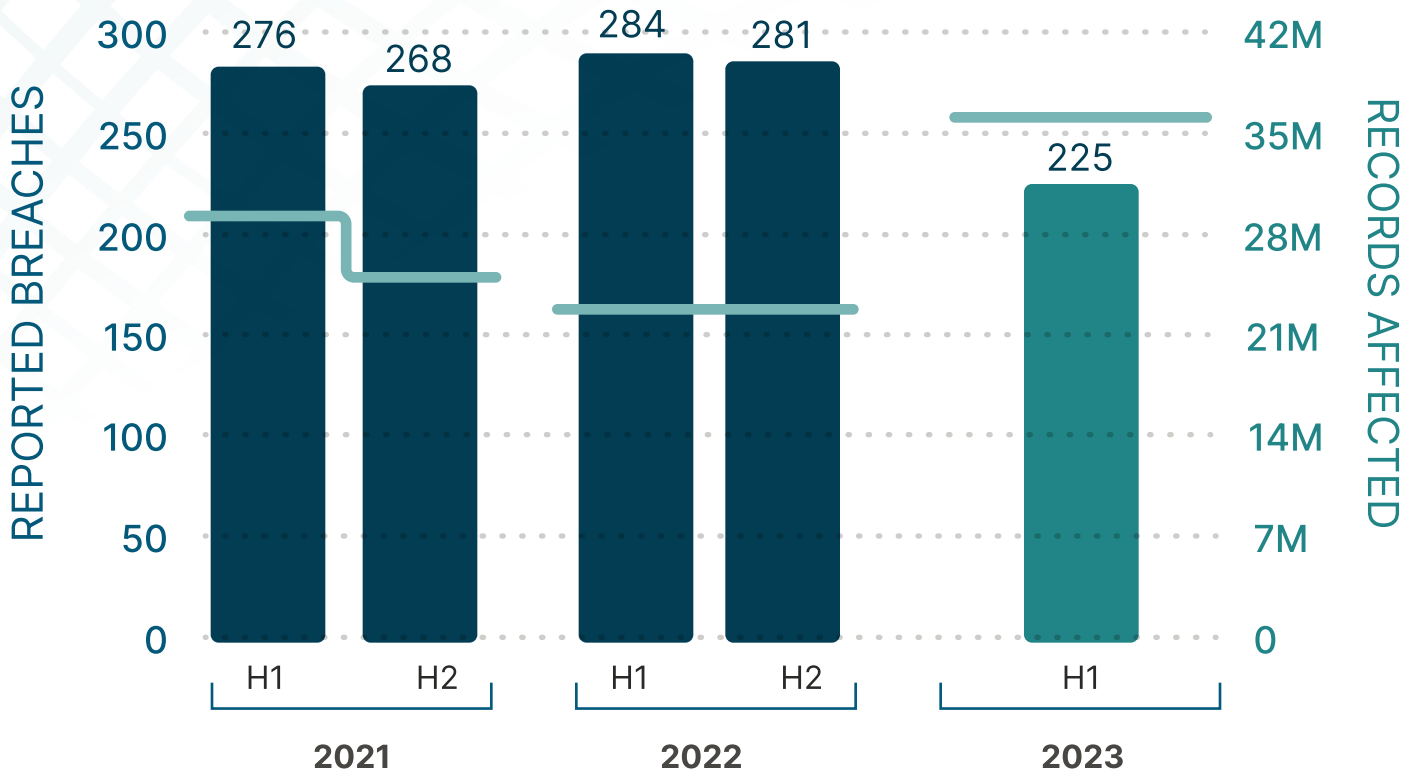
The presence of business associates during hacking and IT incident-related breaches increased from 19% to 25% from the second half of 2022 to the first half of 2023.

HACKING/IT INCIDENTS-BREACHES BY COVERED ENTITY TYPE

The number of people impacted by hacking and IT incidents has reached a concerning 36 million in the first half of 2023. This is already on track to surpass the total of 46 million individuals affected in all of 2022. Out of the 36 million, 46% were affected by breaches at healthcare providers, while 44% were attributed to business associates. The remaining 10% were connected to health plans.

The frequency of hacking and IT incidents impacting healthcare providers fluctuates over half-year periods, with 22 million affected in the second half of 2021, 17 million in the first half of 2022, 9 million in the second half of 2022, and 17 million again in the first half of 2023.

REPORTED HACKING/IT INCIDENTS & RECORDS AFFECTED



Similarly, the number of individuals impacted by hacking and IT incidents at business associates varies based on the occurrence of mega-breaches. The figures stand at 13 million in the first half of 2021, 3 million in the second half of 2021, 5 million in the first half of 2022, 12 million in the second half, and 16 million in the first half of 2023.

The percentage of hacking/IT incidents with a business associate present has remained relatively stable over the past few years at roughly one third of breaches.

Out of the individuals impacted by hacking/IT incidents, 46% had a business associate present, while 54% did not. A total of 17 million people were affected by a business associate, while 19 million were affected without.

HACKER ENTRY POINTS

The majority of cyber-attacks are targeted at network servers, where valuable data is stored. In the first half of 2023, there were 173 hacking/IT incidents that could be traced back to network breaches, while email breaches accounted for 42 incidents. Other sources such as desktops, laptops, and electronic medical records systems had a negligible number of incidents, ranging from 2 to 4.

HACKING/IT INCIDENTS-BREACHES BY LOCATION

Most hacking/IT incidents in the first half of 2023 were caused by network server breaches, accounting for 77% of all incidents. Email-related breaches made up 19% of the incidents, while a small percentage (3%) had multiple causes.

In 2019, hackers had previously focused on exploiting email vulnerabilities. At that time, email breaches accounted for a significant 55% of all incidents, while network server breaches were lower at 34%.

Organizations have since improved their defenses against phishing attacks, resulting in a consistent decline in email-related hacks. As a result, hackers have shifted their tactics towards targeting network vulnerabilities.

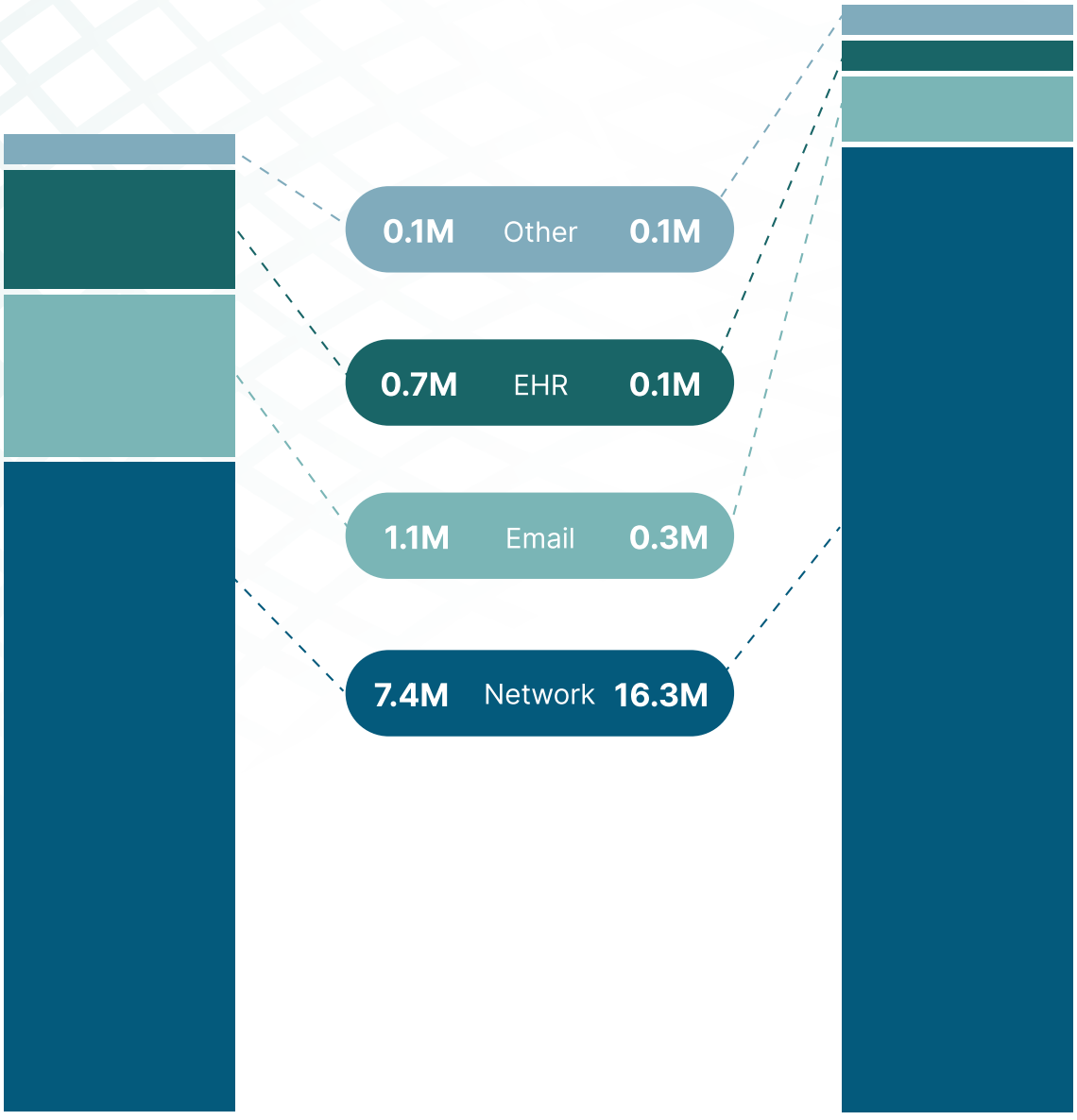
The impact of hacking and IT incidents becomes more evident when we consider the proportion of individuals affected. Network server breaches are responsible for a staggering 97% of individual records affected, while only 2% can be attributed to email breaches.

INDIVIDUALS AFFECTED BY LOCATION

The breakdown of healthcare providers impacted by hacking/IT incidents in the first half of 2023 reveals hospitals as the most targeted at 26%, followed by specialty clinics at 19%. Behavioral health facilities experienced incidents at a rate of 11%, while service and supplies vendors and physician groups both faced threats at 9%. Outpatient facilities, home care, and diagnostic centers each saw incidents at a lower rate of 4%, 3%, and 3% respectively.

INDIVIDUALS AFFECTED BY LOCATION

These figures indicate that hackers are constantly shifting their tactics and targets. Home care facilities, for example, accounted for 18% of incidents in the first half of 2020 but dropped significantly to only 3% in the first half of 2023. Similarly, breaches in specialty clinics decreased by approximately 50% compared to the second half of 2022.



HEALTHCARE PROVIDERS BY TOP MICROSEGMENTS 2023

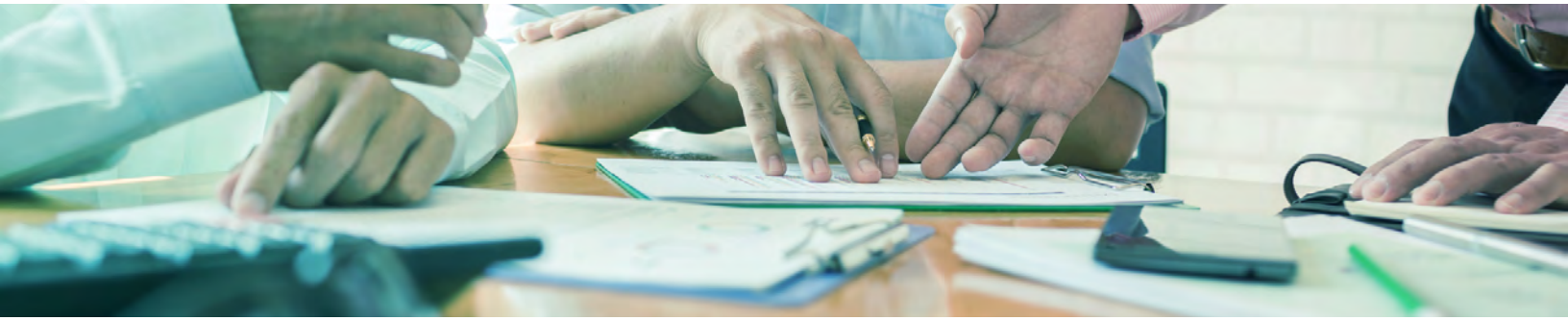
When it comes to individuals affected by hacking/IT incidents within the healthcare provider subset, one or two major hacks can skew the numbers. For example, in the first half of 2021, the percentage of individuals affected in the services and supplies category was 4%; in the first half of 2022 it was 19%, and attributed to the PharMerica attack it skyrocketed to 42% in the first half of 2023.

The Regal Medical Group hack, which affected 3.4 million individual records, pushed the physician group microsegment from 4% in the second half of 2022 to 22% in the first half of 2023.

Enzo Clinical Labs reported a breach involving nearly 2.5 million individuals, pushing the diagnostic segment from 3% in the second half of 2022 to 15% in the first half of 2023.

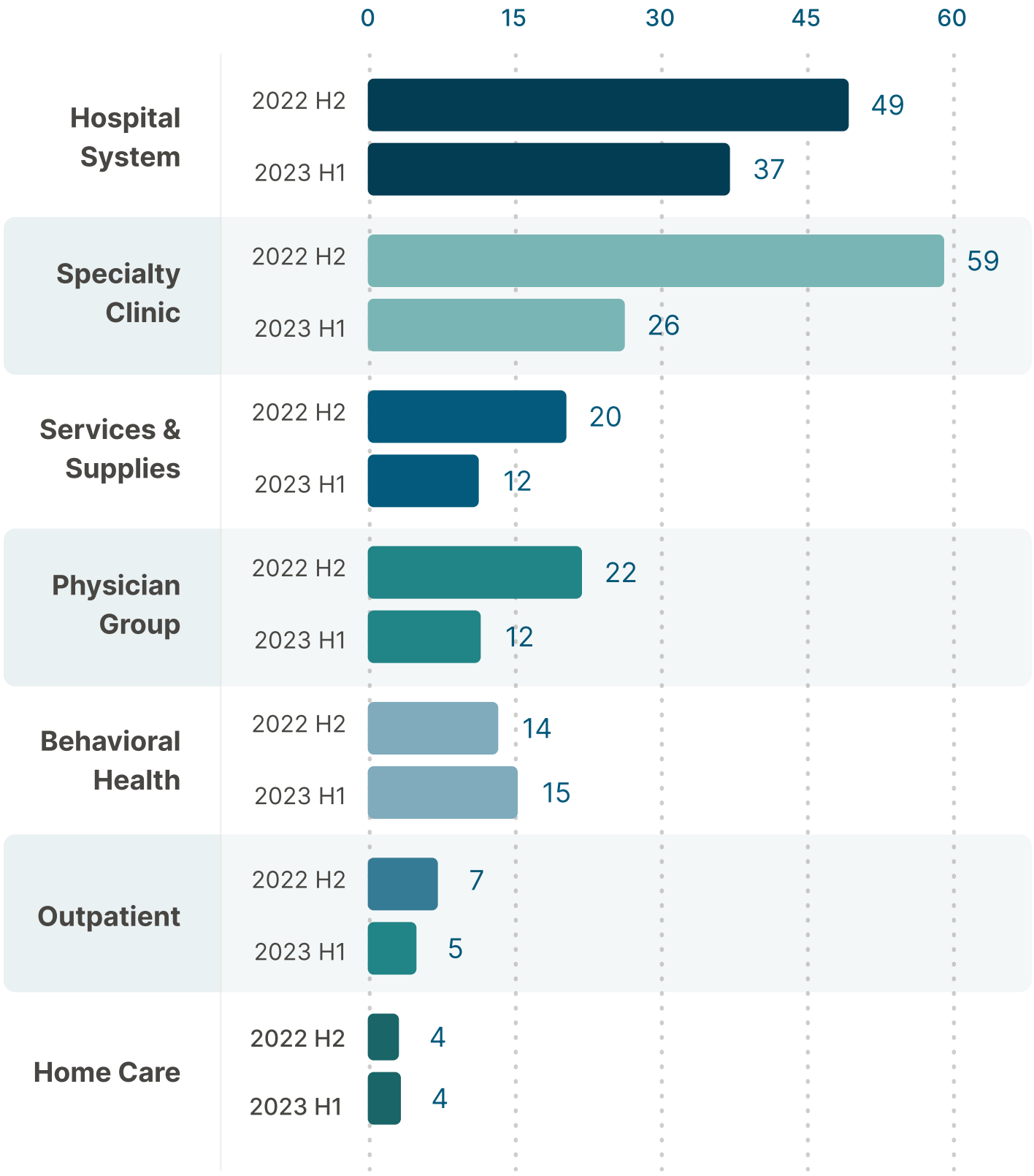
On a positive note, hospital systems only accounted for 10% of individual records affected by hacking IT/incidents in the first half of 2023, down from 33% in the second half of 2022.

Specialty clinics went from 25% in the second half of 2022 to 8% in the first half of 2023.



HEALTHCARE PROVIDERS BY TOP MICROSEGMENTS 2023

Hacking/IT Incidents



WHAT SHOULD HEALTHCARE ORGANIZATIONS DO?

It is crucial for healthcare organizations to remain vigilant as attackers constantly adapt to avoid being hacked. The key takeaway is the importance of preparation, detection, and effective incident response.

To adequately prepare, first start with an incident response plan along with a NIST-CSF based risk assessment with assessment to build a multi-year strategy. It will be helpful to have support from the board and they will appreciate your focus on the most critical or maximum impact for the investment.

For improving detection, make sure to correlate logs so that you know what is normal versus what is anomalous. Logs are labor intensive to maintain and can create a lot of “noise”. To help with alert fatigue, consider SOC-as-a-Service or MDR solutions, like those offered by Critical Insight.

Effective Incident Response relies on knowing what to do when an incident occurs, before it occurs. Playbooks help establish who should do what and when, so that when things go wrong, you know how to address them.

And in doubt, have a trusted incident response provider ready to assist, 24×7, instead of relying on an unknown provider that’s just available at the moment of breach.

Lastly, a robust focus must be placed on safeguarding third-party vendors, business associates, and suppliers from vulnerabilities. Tracking the cyber hygiene of your most critical partners is important to maintaining a more secure environment.

While some organizations may have the resources to develop these capabilities internally, those with budget constraints, staffing limitations, or missing specialized cybersecurity skills can partner with an expert cybersecurity service provider.

Critical Insight provides services to help healthcare organizations achieve compliance, test their security posture, and provide around-the-clock response to any breach attempts. Learn more at criticalinsight.com

American Hospital Association™
Preferred Cybersecurity Service

Critical Insight is an American Hospital Association preferred provider of cybersecurity services, including Managed Detection and Response (MDR).

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.

Brett Shorts

Brett has over 20 years of experience using research and analytics to drive business decisions and process improvement. He is currently the Director of Sales and Marketing Operations at Critical Insight.