JULY-DEC
2022

HEALTHCARE BREACH REPORT

Critical Insight

Security Research and Data Analysis

TABLE OF CONTENTS

Overview

The number of data breaches affecting healthcare providers declined in the second half of 2022, consistent with a downward trend over the past two years. But a deeper dive into the data reveals that current breach totals are still higher than pre-pandemic levels, breaches are affecting more individuals, and hackers are shifting their tactics to attack weak links in the healthcare system supply chain, most notably attacking Electronic Health Record systems.

These are among the key insights from Critical Insight's analysis of breach data reported

to the US Department of Health and Human Services (DHHS), detailed in this report. Organizations that handle healthcare data are required to report breaches that expose more than 500 individual records within 60 days of discovering the breach.

Here are the major takeaways from data collected over the second half of 2022:

Breach numbers are down. Total breaches dropped 9% between the first six months of 2022 and the second half of the year. Breaches have been declining since a high-water mark at the height of the pandemic; from 393 breaches in the second half of 2020 to 313 in the latest reporting period.

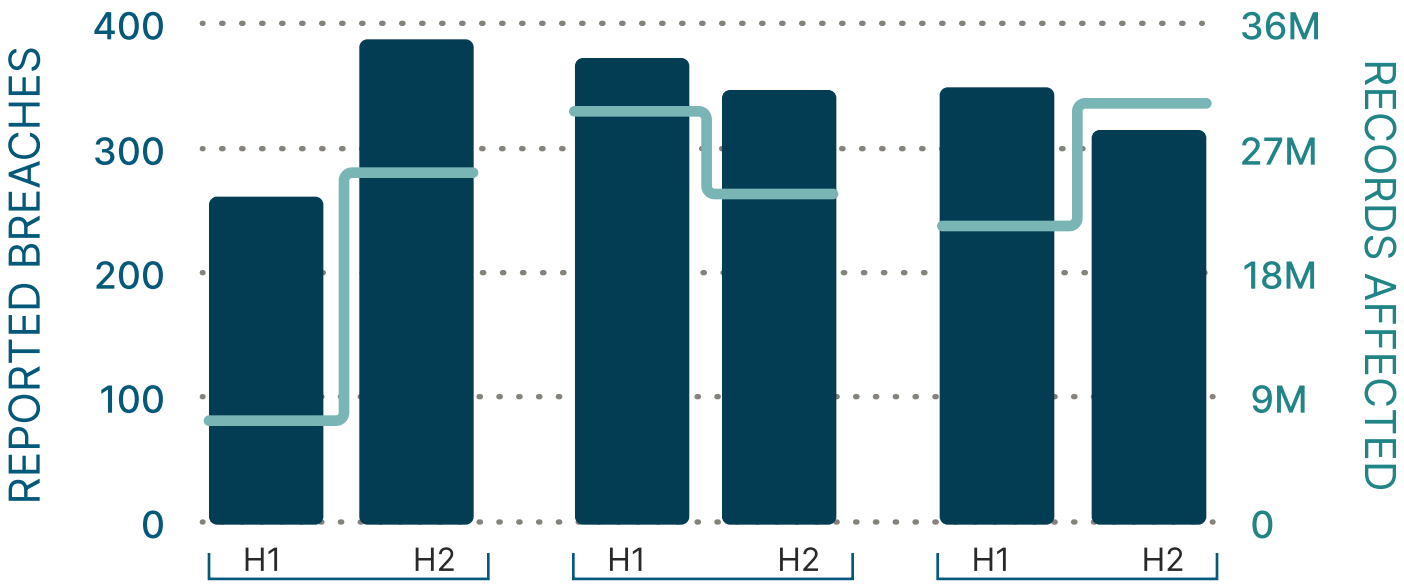
Records affected are up. The number of individual records exposed by breaches skyrocketed by 35% in the second half of 2022 to hit 28 million. In other words, fewer breaches, but larger breaches, reflecting consolidation within the industry and the evolving tactics of attackers.

> "Breaches affecting healthcare systems is trending downward, but breaches are affecting a growing number of individuals."

Hacking remains high. The vast majority of data breaches are due to hacking. Healthcare organizations have done a relatively good job shoring up their policies around the proper handling and storage of medical records. Hacking accounted for 79% of all incidents and 84% of individual records exposed in 2022.

Attackers continue to attack hospitals, but have found increasing success targeting business associates, third-party vendors such as electronic medical record providers, lawyers, accountants, billing companies and medical device manufacturers. In the second half of 2022, more records were exposed due to breaches at business associates (48%) than actual healthcare providers (47%). Attacks against EMR systems, which were non-existent in past years, spiked to 7% in the first half of 2022 and 4% in the second half of 2022.

REPORTED BREACHES & RECORDS AFFECTED



	H1	H2	H1	H2	H1	H2
Breaches	269	393	367	344	345	313
Individuals	8.3M	26.1M	28.0M	25.4M	21.1M	28.5M

In one of the most notable breaches of 2022, CommonSpirit Health, the nation's second-largest nonprofit healthcare system, reported a ransomware attack that impacted more than 600,000 patient records.

In response to the attack, CommonSpirit took its entire EMR system offline so it could investigate the breach and make sure that enhanced security measures were in place before it brought the system back online.

As a result, the EMR system was not available to healthcare providers who had to abruptly cancel appointments with patients.

CommonSpirit said it was able to trace the breach back to an unauthorized third party who gained access to certain portions of CommonSpirit's network.

THE BREACH LANDSCAPE

The total number of reported breaches took a sharp drop in the second half of 2022, from 345 in the first half of the year to 313 – a solid 9% reduction. Over the last four six-month reporting periods total breaches declined from 367 to 313.

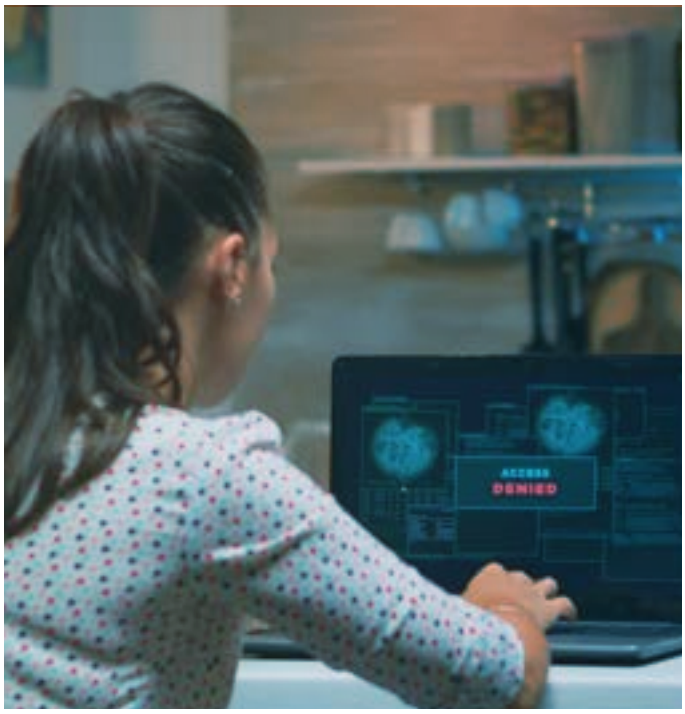
On an annual basis, breaches for 2022 totaled 658, which is 7% lower than the 711 from 2021 and lower than 2020, when there were 662 reported breaches. Still, current breach numbers remain higher than pre-pandemic levels – there were only 506 reported breaches in 2019.

While the total number of breaches declined over the latest reporting period, the number of individuals affected jumped sharply, from 21.1 million records to 28.5 million records, a 35% increase. Except for the outlier period in the second half of 2019, when there were two mega-breaches that exposed more than 10 million records each, the second half of 2022 represented the highest number of individuals affected over the past four years.

35% Increase in total records affected in the second half of 2022

However, full-year totals show that 6% fewer individuals were affected in 2022, compared to 2021. Those full year numbers are 53.4 million for 2021 and 49.6 million in 2022.

Since the total number of breaches was down in the second half of 2022 and the total number of individuals affected was higher, the ratio of individuals affected per breach also soared. In the second half of 2022, 91,028 individuals were affected per breach, compared to only 61,246 in the first half of 2022.



WHAT ARE THE CAUSES OF DATA BREACHES?

The reporting process identifies five possible types of breaches – hacking/IT incidents, unauthorized access/disclosure, theft, loss and improper disposal.

Not surprisingly, hacking/IT incidents were listed as the cause in the vast majority of breaches – 78% in the second half of 2022. Unauthorized access/disclosure was the second-most cited type at 16%,

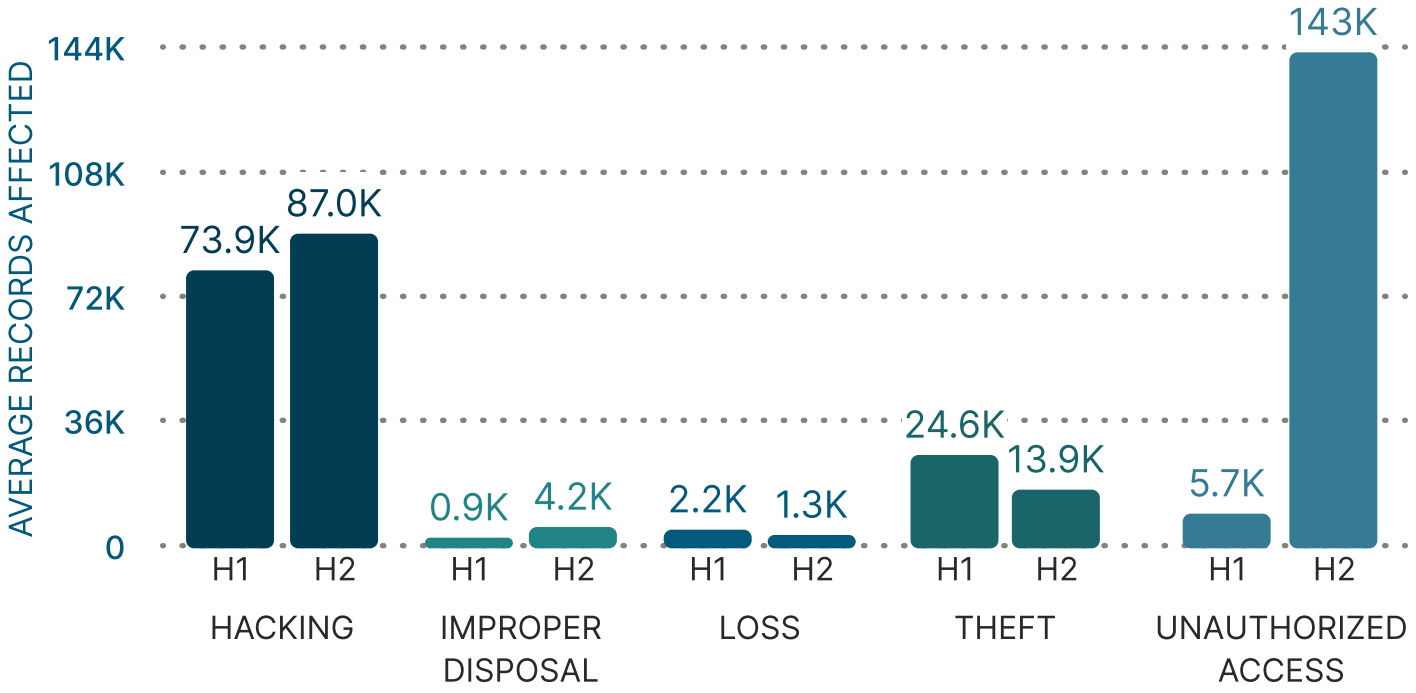
with theft at 3.5%, loss at 2% and improper disposal at under 1%.

Looking at long-term trends, the percentage of hacking/IT incidents has risen from 61% in 2019 to 79% in 2022, while the percentage of unauthorized access/disclosure has dropped from 27% in 2019 to 15% in 2022.

Theft has been cut dramatically; from 7.5% in 2019 to 3.3% in 2022.

In raw numbers, reported hacking incidents went from 278 to 244 between the first and second halves of 2022. There were 50 reports of unauthorized

AVERAGE RECORDS AFFECTED BY BREACH TYPE IN 2022



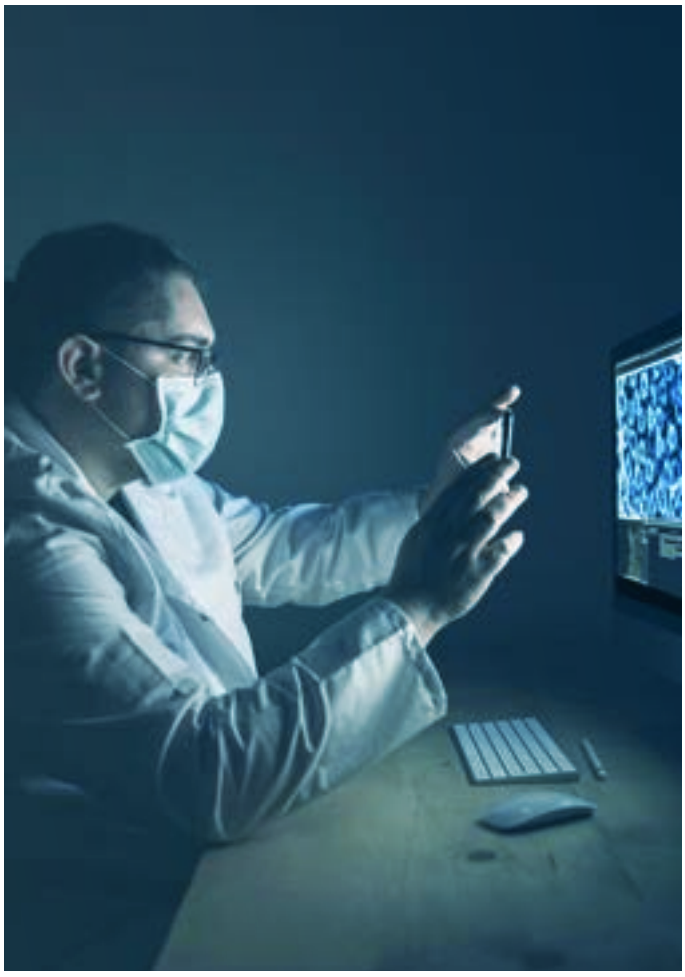
access/disclosure, 11 reports of theft, seven reports of loss and only one case of improper disposal.

Unauthorized access/ disclosure now, on average, effects more records per breach than any other breach type.

Switching to the number of individuals affected by breach types, hacking/IT incidents accounted for 84% of all affected individuals in 2022. That's actually down from 96% in 2021.

The sharp reduction in the percentage of individuals affected by hacking/IT incidents reflects the rise in the number of individuals affected by unauthorized access/disclosure. On average, the number of individuals affected per unauthorized access/disclosure breach spiked from 5,700 in the first half of 2022, to over 143,000 in the second half. By comparison, the average individuals affected per hacking breach grew from 73,900 to 87,000 over 2022.

The surge in records affected by unauthorized access/disclosure was caused by three large breaches, totaling 5.9 million individuals.



WHO IS GETTING BREACHED?

If you're a hacker looking for patient data, the healthcare provider is the most obvious and direct target. That premise is borne out by the fact that 69% of breaches in the second half of 2022 involved healthcare providers. But hackers are also stepping up their attacks on third-party business associates.

Since 2019, the percentage of breaches at healthcare providers has slowly declined, from 81% in the second half of 2020 to 72% in the second half of 2021 to 69% in the second half of 2022.

At the same time, the percentage of breaches associated with business associates has trended upward, from 9% in the second half of 2020 to 13% in the second half of 2021 to 19% in the second half of 2022.

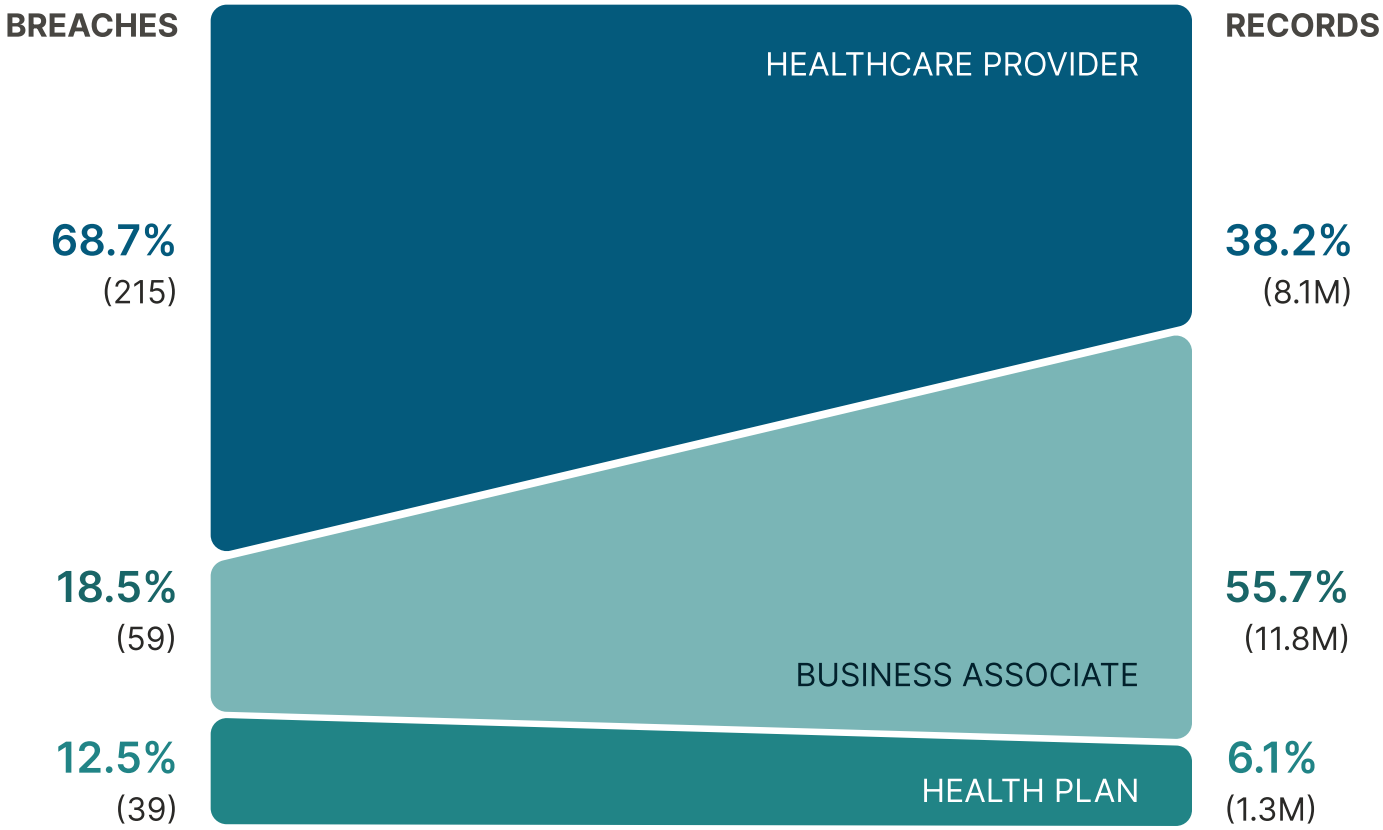
Looking at full-year numbers, breaches at healthcare providers declined from 78% in 2020 to 72% in 2021 to 71% in 2022.

Conversely, the percentage of breaches linked to business associates increased from 11% in 2020 to 13% in 2021 to 17% in 2022.

"Breaches associated with business associates involve more records per breach."

Breaches associated with health plans remained relatively stable over time: 12% in 2019, 11% in 2020, 15% in 2021 and 12% in 2022.

BREACHES INVOLVING BUSINESS ASSOCIATES



Historically, breaches associated with business associates involve more records per breach. While business associates-related breaches accounted for 19% of breaches in H2 2022, they affected over 55% of individuals, driven by four breaches affecting more than 1 million individuals each.

Breaches associated with healthcare providers accounted for 69% of individuals, and health plans accounted for the remaining 13% in H2 2022.

The reporting system makes a distinction between direct attacks against business associates and attacks in which the hackers eventually hit a

healthcare provider, but the initial entry point for the attack was a business associate. This evolving tactic among hackers presents a challenge for frontline healthcare organizations.

Looking specifically at the subset of breaches linked to hacking, the number of hacking/IT incidents dropped from 278 in the first half of 2022 to 244 in the second half of the year.

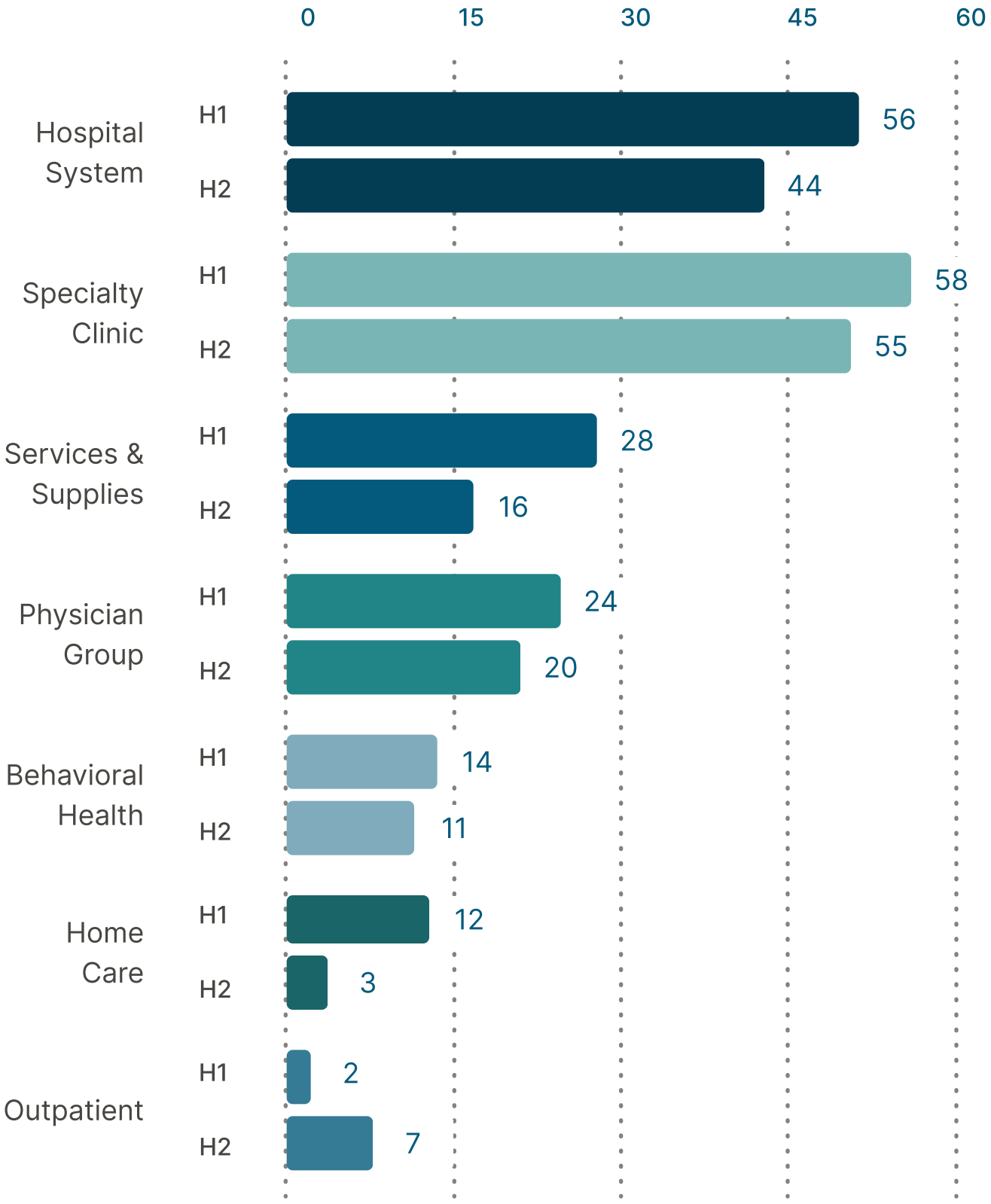
Healthcare providers accounted for 70% of all hacking incidents in the second half of 2022, followed by business associates at 19% and health plans at 11%.

Hacking/IT incidents on healthcare providers dropped from 278 in the first half of 2022 to 244 in the second half of the year.

Since hacks linked to business associates result in higher numbers of individuals affected, business associates accounted for 39% of individuals affected by hacking incidents, with healthcare providers accounting for 55%, and health plans at 6%.

There were 171 hacking/IT incidents reported in the second half of 2022. Drilling down into the specific targets within the healthcare system, specialty clinics topped the list with 55 reported hacking incidents (32%), followed by hospital systems at 44 (26%), physician groups at 20 (12%), services and supplies at 16 (9%), behavioral health at 11 and outpatient care at 7 (6%).

HACKING/IT BREACHES PER MICROSEGMENT, 2022



HOW ARE HACKERS GETTING IN?

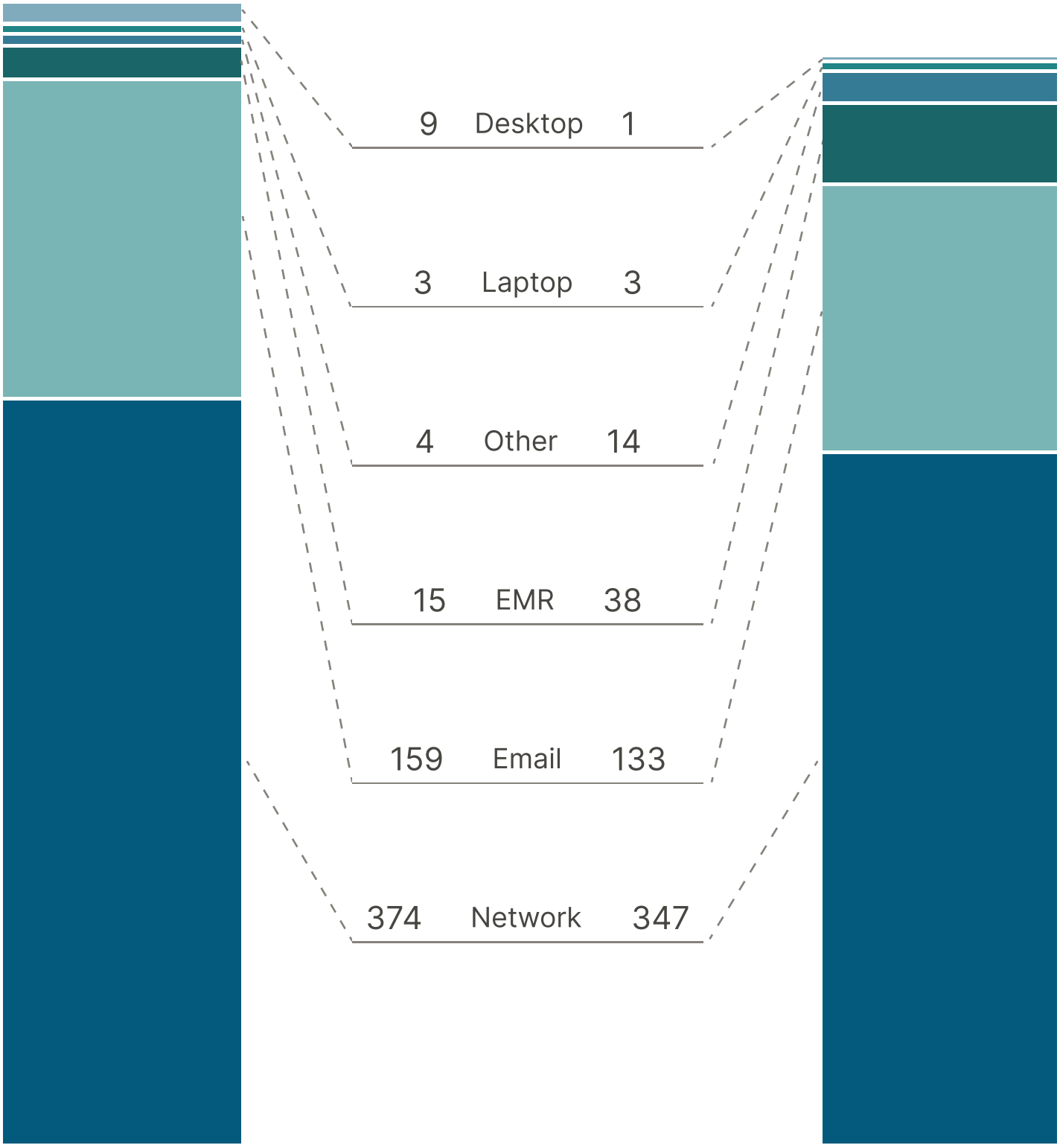
Defending against cyberattacks requires an understanding of how records are being exposed. Servers were linked to 71% of incidents in the second half of 2022, up from 58% in the first half of 2022. Email was listed in 20% of incidents in the second half of 2022, down from 30% in the first half of 2022. Breaches linked to the hacking of Electronic Medical Record (EMR) systems were negligible prior to this year, when they spiked to 7% in the first half of 2022 and 4% in the second half of the year.

For the full year 2022, EMR-related breaches accounted for 6 million individual records exposed, or 8% of all individual records exposed in the first half of 2022 and 7% in the second half of the year.

In addition to the breach at CommonSpirit Health, 2.2 million patient records were exposed in a breach at Connexion Software, a company that provides pediatric EMR software to 119 healthcare providers. Connexion reported that hackers were able to access an offline set of ERM data, rather than the live data, so healthcare services were not impacted.

However, the exposed records included Social Security numbers, patient demographic information (i.e., name, address, email address, and date of birth), health insurance information, medical and treatment information, billing or claims information,

DISTRIBUTION OF BREACHES BY LOCATION



Critical Insight

https://criticalinsight.com

and possibly information about a parent, guardian, or guarantor of patients.

Network servers were the jackpot for hackers, accounting for 90% of individual records breaches, followed by email at 6%, EMR at 3%.

For example, Shields HealthCare Group, a third-party vendor that provides MRI, PET, and CT scan services, reported in June that a network server was breached, exposing 2 million patient records tied to 60 health care providers.

Similarly, One TouchPoint, which provides marketing, printing and mail services to healthcare providers, reported in August that threat actors had accessed several network servers and launched a ransomware attack that affected 4.1 million individual records at 30 health plans.

"Breaches linked to EMR systems in 2022, affecting nearly 6 million individuals in the second half of this year."

WHAT CAN HEALTHCARE ORGANIZATIONS DO?

Now is a good time for healthcare companies to make sure they are focusing on preparation, detection and incident response. Companies seeking to improve their cybersecurity posture can do so by building capability internally, or by working with a partner who can provide expert cybersecurity staff and services.

In addition to protecting themselves, healthcare companies must ensure that all third-party vendors, business associates and suppliers in their networks are following sound security procedures.

Critical Insight provides Cybersecurity-as-a-Service to help you achieve compliance, test your security posture and provide instant, around-the-clock response to any breach attempts.

Critical Insight's healthcare consulting team helps organizations defend against the types of attacks listed in this report. An excellent risk assessment is the key to setting up a successful security journey, followed by a Third-Party Risk Management program. Knowing that a skilled attacker will breach the perimeter, a strong incident response plan, tested by tabletop exercises is necessary.

To know when to declare an incident, healthcare organizations need to know immediately when there is a security event, creating a need for 24×7×365 Critical Insight Managed Detection and Response (SOC services) with the ability to rapidly quarantine impacted assets limiting the impact of the attack. Critical Insight works with your existing infrastructure to get you protected against breaches quickly and effectively.

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.