Critical Insight

HEALTHCARE BREACH REPORT

Jan-June 2022

Security Research and Data Analysis

TABLE OF CONTENTS

© 2022 Critical Insight Inc.

Overview

The total number of data breaches affecting healthcare systems has receded since the high-water mark set during peak COVID, but this is no time for organizations to let their guards down. The number of successful hacking incidents ticked higher and remains at an unacceptably high level, with hackers shifting their methods to exploit vulnerabilities associated with third-parties and smaller healthcare facilities.

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.

© 2022 Critical Insight Inc.

Here are the major takeaways from data collected over the first six months of 2022:

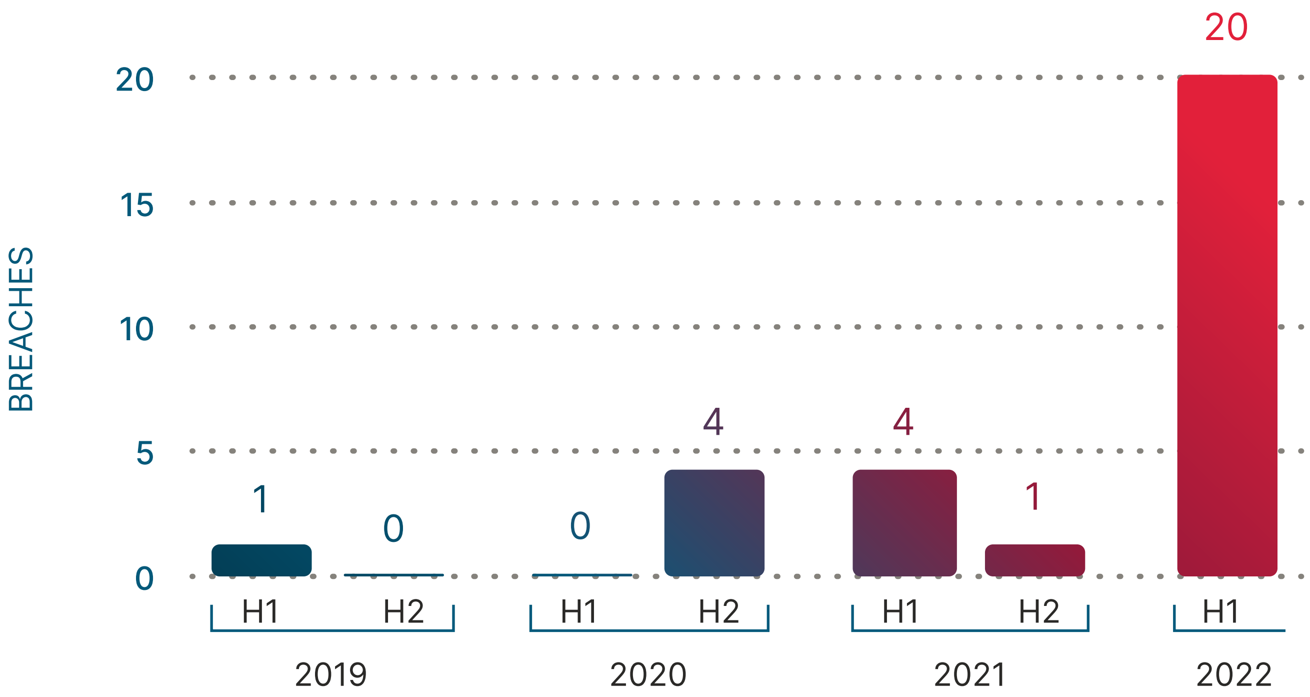
- The total number of breaches is down 6% when comparing the first half of 2022 with the first half of 2021. Total breaches have declined for three consecutive six-month periods, and 2022 may see the first decline in annual breaches since Critical Insight began tracking the data. But, the yearly total is still expected to be above pre-pandemic levels.

- Attackers seem to be shifting their focus away from large healthcare facilities, big targets that might yield the most data but also tend to have the strongest defenses, to smaller hospital systems and specialty clinics that might not have the same level of security preparedness, staff size, or budget. Hackers are also targeting physician groups. The number of attacks on physician groups has increased from 2% of total breaches in the first half of 2021 to 12% in the first half of 2022.

© 2022 Critical Insight Inc.

- Consolidation within the industry (multiple healthcare systems using the same electronic medical record (EMR) vendors, for example), has led to millions of exposed records as a result of attacks against third-party service providers. Electronic medical records (EMR) systems have emerged as a serious target for hackers, and increasingly breaches are occurring on third-party business associates, rather than on providers themselves.

INDIVIDUAL REPORTED INCIDENTS FROM EMR BREACHES



Key Finding: Hacking incidents on EMR systems increased to 20 incidents in the first half of 2022, and now represent 8% of all hacking breaches.

© 2022 Critical Insight Inc.

TOTAL BREACHES ARE DECLINING

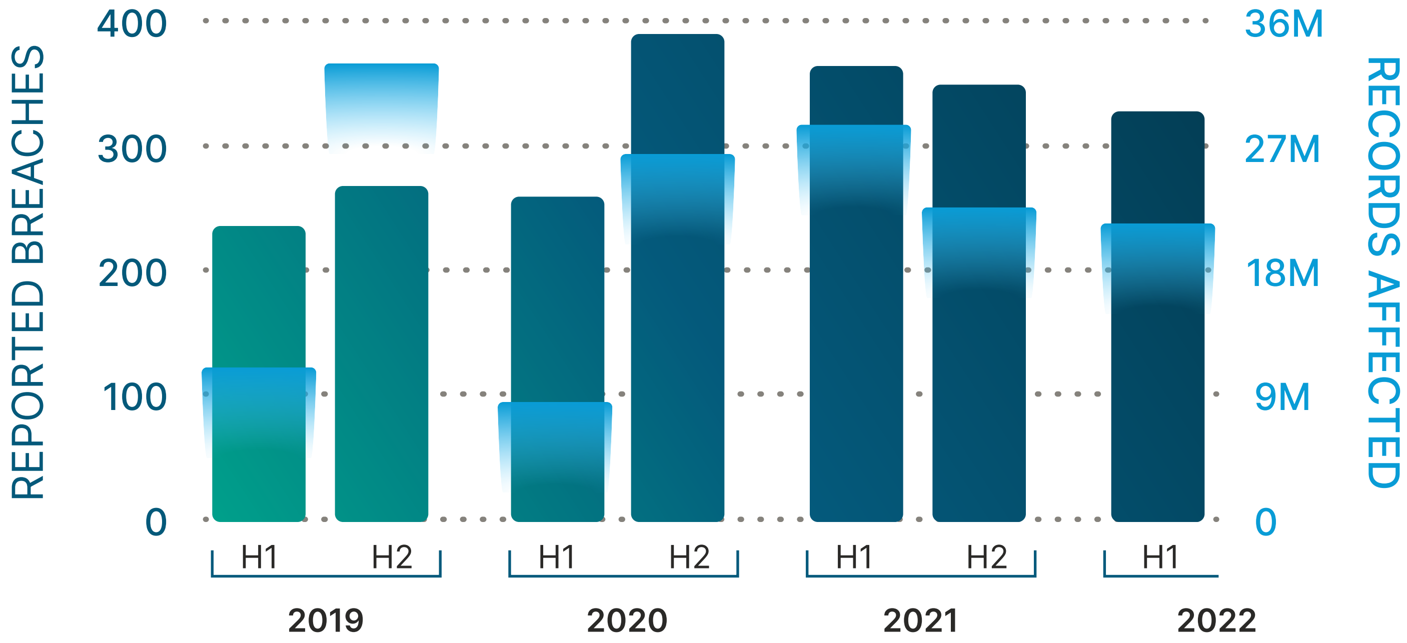
The number of reported breaches crested during the second half of 2020 when organizations were so distracted by the pandemic that attackers had more opportunity to breach their defenses.

Since then, the total number of breaches has slowly but steadily declined in each half-year period, from the peak of 393 in the second half of 2020 to 324 in the first half of this year.

324 breaches, however, is still significantly higher than a typical half-year breach count at pre-pandemic levels. If we assume that the trend of declining breaches will continue for the rest of 2022, we can estimate that total breaches for this year will be lower than 2020 or 2021, but still higher than 2019.

© 2022 Critical Insight Inc.

REPORTED BREACHES & RECORDS AFFECTED BY HALF YEAR



	H1	H2	H1	H2	H1	H2	H1
Breaches	233	273	269	393	367	344	324
Records	11.5M	33.5M	8.2M	26.2M	27.6M	22.2M	19.9M

Key Finding: Both the number of breaches and records affected have decreased for the third consecutive half year.

The total number of breaches is important, but even more critical is the number of individual patient or client records affected by the breaches. The latest numbers are encouraging: roughly 20 million individuals were affected in the first half of

2022, representing the third consecutive period of decline, a 10% drop compared to the prior six-month period and 28% less than the first half of 2021.

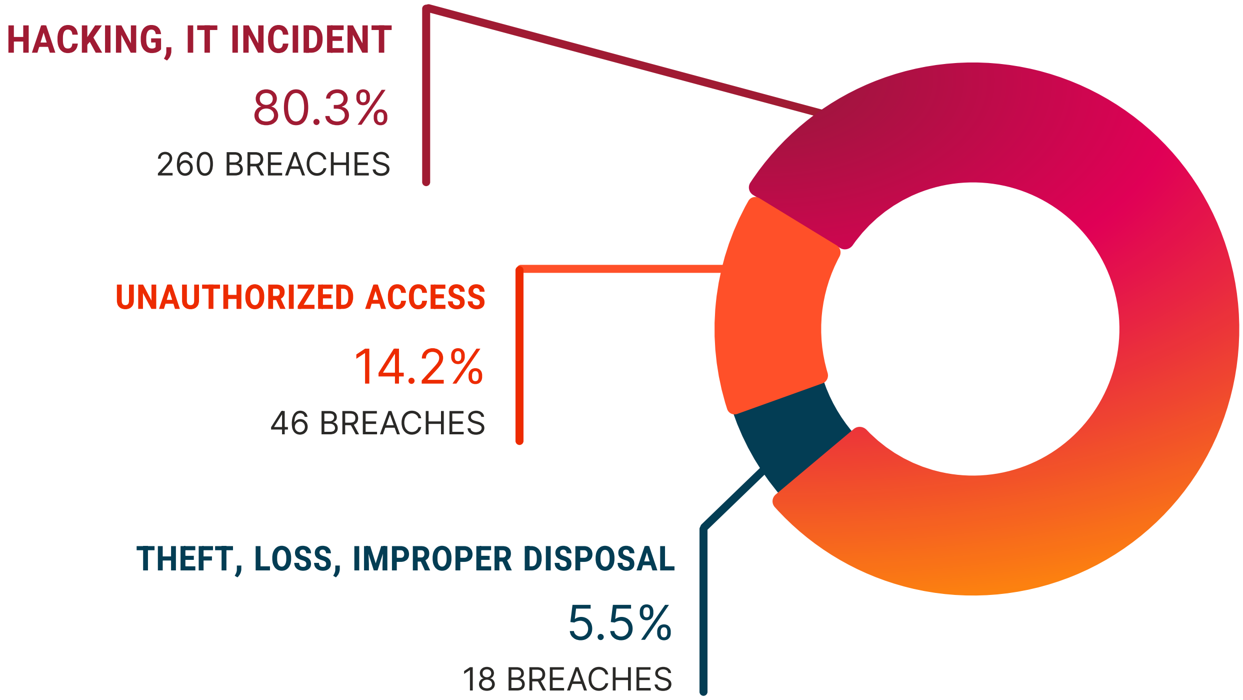
As has become typical, there were several mega-breaches during the first six months of 2022. The Eye Care Leaders EMR breach exposed more than 2 million records. Shields Health Care Group in Quincy, Mass., which provides management and imaging services to more than 50 healthcare facilities, also reported a breach involving 2 million individuals.

Partnership HealthPlan of California, a third-party entity that administers Medicare benefits, suffered a breach that affected 850,000 individuals.

And Arizona's Yuma Regional Medical Center disclosed that it was the victim of a ransomware attack that exposed the Social Security numbers and other personal information of 700,000 individuals.

© 2022 Critical Insight Inc.

2022 BREACHES BY TYPE



Over eighty percent of breaches were caused by hacking/IT incidents, up from 61% in 2019. While improper disposal or loss of patient records are serious, they don't expose individuals to having their personal data sold on the Dark Web. Hacking is responsible for 97% of the reported breaches that actually affect individuals.

Key Finding: Hacking/IT incidents make up over 80% of breaches, and are the only breach type that has grown in number over the last half year.

© 2022 Critical Insight Inc.

WHO IS GETTING HACKED?

If we divide healthcare entities into three main buckets – healthcare providers, health plans and business associates - healthcare providers account for a vast majority of breaches but are trending downward, decreasing from 269 breaches in the first half of 2021 to 238 breaches in the first half of 2022. In the last half year, business associates surpassed health plans as the second-most breached entity.

A "business associate" is an entity, typically a vendor, that performs activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

Examples include practice management services, electronic medical record providers, lawyers, accountants, IT consultants, billing companies, cloud storage services, web hosts, medical device manufacturers, and more.

The percentage of breaches linked to business associates has climbed from 10.3% in 2019 to 14.5% in the first half of 2022. And importantly, due to consolidation within the healthcare industry, the average number of individuals affected by a breach is actually significantly higher for business associates (97,000 records per breach) than for healthcare providers (59,000 records per breach).

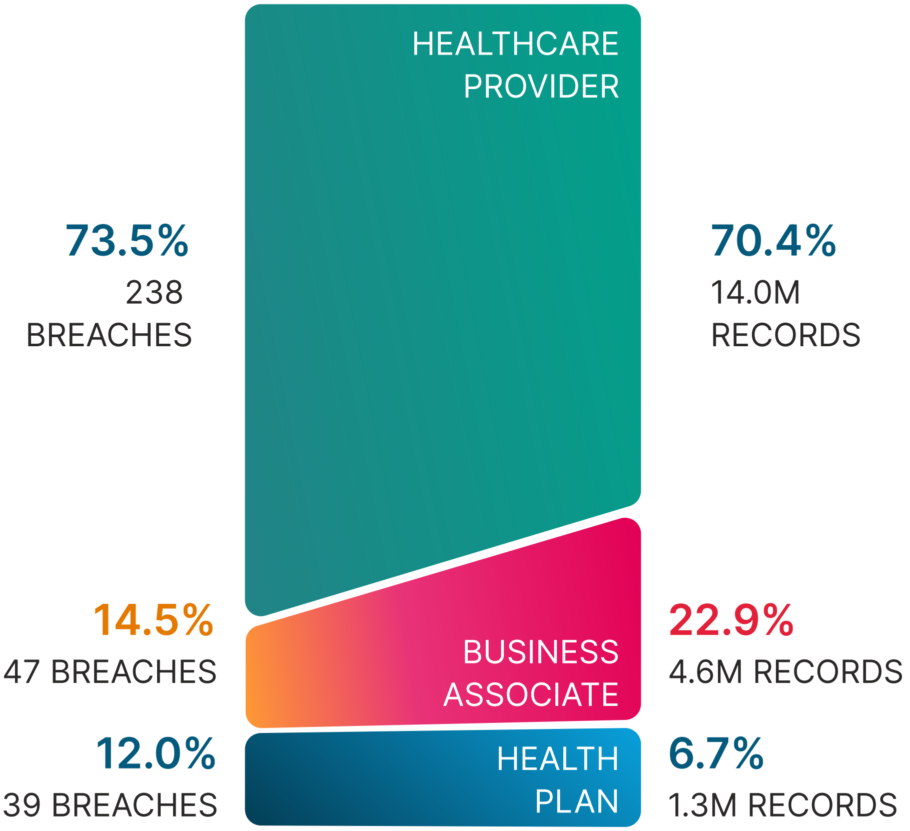
Drilling down into healthcare provider micro segments, specialty clinics emerge as the top source of data breaches at 31%, up from 23% in 2021, and from only 20% in 2019. Hospital

© 2022 Critical Insight Inc.

systems come in a close second at 29.6%; clearly, attackers are targeting smaller specialty clinics that might not have the same level of security as a large hospital, even though there may be fewer records to expose.

Similarly, the category of services and supplies (pharmacies, medical supply companies, provider alliances) accounted for 14% of breaches in the first half of 2022, up from 10% in the second half of 2020. In fact, the percentage of breaches linked to service and supplies has risen every reporting period since the second half of 2019, when it was only 5% of total breaches.

2022 BREACHES INVOLVING BUSINESS ASSOCIATES



Key Finding: Business associate breaches are rising in frequency, and involve far more records per breach than other healthcare entity.

Critical Insight

https://criticalinsight.com

© 2022 Critical Insight Inc.

CAUSES AND EFFECTS OF HACKING INCIDENTS

Since hacking/IT incidents can result in loss of money, possible interruption of critical services in a ransomware scenario, as well as long-term business losses due to reputational damage, it’s important to analyze the causes and effects of these types of breaches.

Hacking/IT breaches associated with electronic medical records (EMR) systems skyrocketed from only a single reported incident in the second half of 2021 to 20 in the first half of 2022. With 19 of those incidents related to the massive Eye Care data breach, the big takeaway is that even though a successful hack may directly target one vendor, the impact is felt among many providers who may use that vendor.

Breaches associated with network servers have represented a majority of hacking/IT incidents by location since the first half of 2020, but have declined from a peak of 67% of hacking/IT incidents in the first half of 2021 to 57% in the first half of 2022. But, EMR-related breaches soared from zero in the first half of 2020 to nearly 8% of all breaches in the first half of 2022. Clearly, hackers have found a new target in the third-party organizations that manage and store medical records.

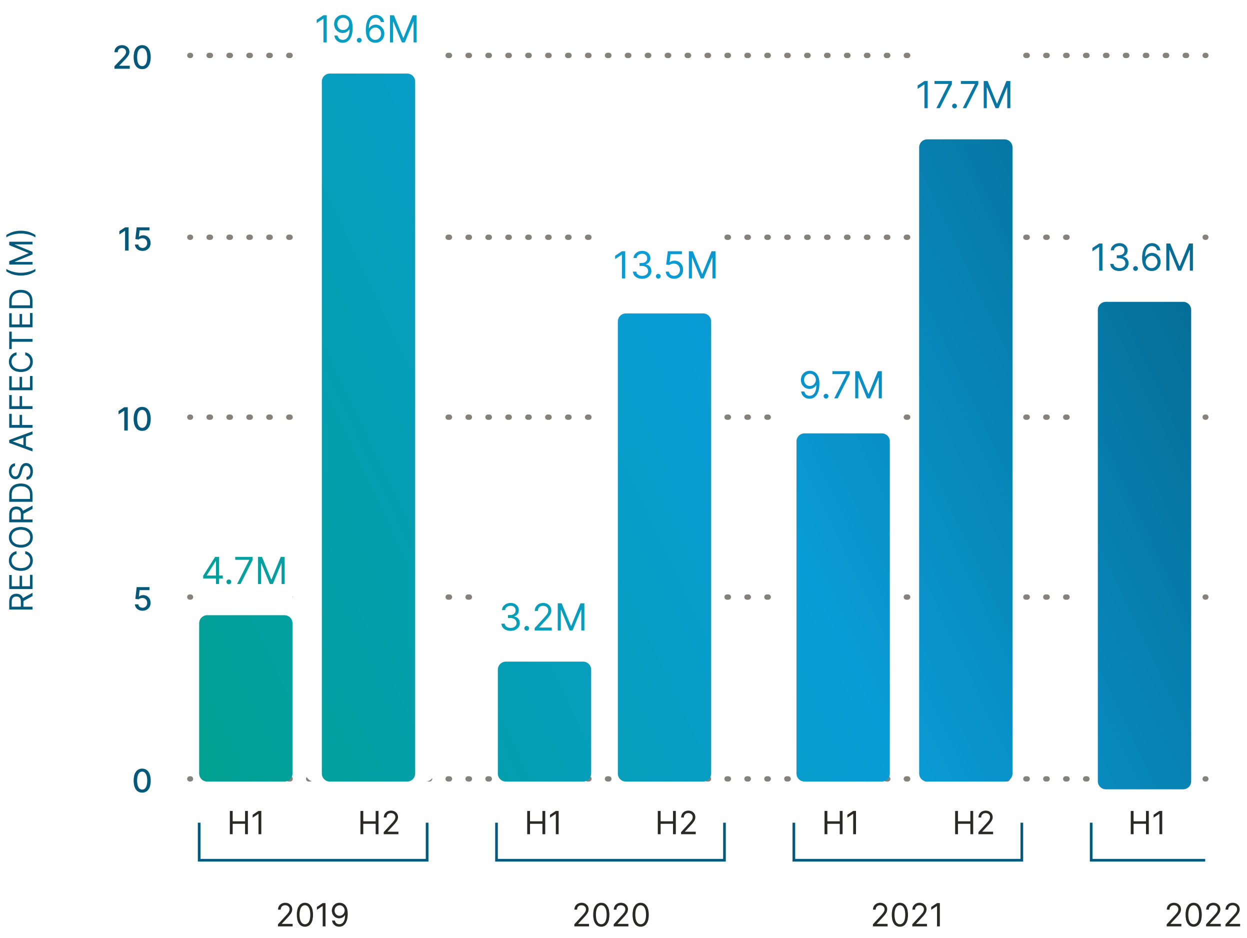
© 2022 Critical Insight Inc.

While the raw number of hacking/IT incidents increased only 2% from the second half of 2021 to the first half of 2022, the impact has been disproportionately significant in terms of records affected, with hacking incidents associated with healthcare providers thus far in 2022 already affecting nearly as many individuals as all of 2020.

Individuals affected by hacking/IT incidents accounted for 70% of all individuals affected in the first half of 2022, a significant increase from the 55-60% range in 2019-2021.

© 2022 Critical Insight Inc.

HACKING INCIDENTS AFFECTING HEALTHCARE PROVIDERS



Key Finding: There have been significantly more records exposed by breaches in the second half of the year, while the first half of year baseline has crept upward. This could indicate risk of a record number of affected individuals in the second half of 2022.

© 2022 Critical Insight Inc.

WHAT CAN HEALTHCARE ORGANIZATIONS DO?

As healthcare companies attempt to return to a post-COVID version of normalcy, it is important to remember that hackers are becoming more agile and opportunistic, constantly looking for new targets, such as EMR systems.

Healthcare organizations are likely to look quite different today than pre-COVID. For example, administrators and other support staff that don't need to physically be at the healthcare facility might have settled into a hybrid work schedule. This creates potential security vulnerabilities.

Similarly, the increased use of telemedicine and Zoom meetings creates openings for hackers.

And, the pandemic has caused supply chain disruptions, which have resulted in healthcare organizations scrambling to find new suppliers who might not have been sufficiently vetted due to the emergency nature of the situation.

Now is a good time for healthcare companies to make sure they are doing the three things that matter most: preparing for an attack, detecting attacks quickly, and responding rapidly and effectively. Companies seeking to improve their cybersecurity can do so by building capability internally, or by working with a partner to provide expert cybersecurity staff and services.

© 2022 Critical Insight Inc.

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. Taking these steps and preventative measures helps to protect the entire healthcare industry.

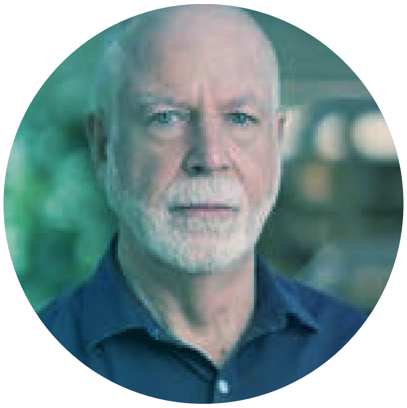
Critical Insight provides Cybersecurity-as-a-Service to help you achieve compliance, test your security posture and provide instant, around-the-clock response to any breach attempts. Critical Insight works with your existing infrastructure to get you protected against breaches quickly and effectively.

© 2022 Critical Insight Inc.

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.

© 2022 Critical Insight Inc.