Critical Insight

Healthcare Breach Report

Jan-June 2021

Security Research and
Data Analysis

Table of Contents

Overview

Data on cyberattacks from the first half of 2021 shows criminals are changing targets within the healthcare ecosystem, with breaches increasing for outpatient facilities and business associates. The data also shows some long-term trends continuing, with overall attacks on an upward trend.

At the start of the year, the U.S. was just beginning its struggle with the COVID-19 vaccine rollout. As the healthcare industry tried to meet the dynamic demands of the pandemic, it did so with 2020 behind it, a year memorable for both COVID-19 and an explosion of ransomware attacks. As 2021 began, organizations focused on the immense security and compliance needs because of direct attacks, supply chain attacks, telehealth, and the increased outsourcing of business operations.

"...with 2020 behind it, a year memorable for both COVID-19 and an explosion of ransomware attacks....."

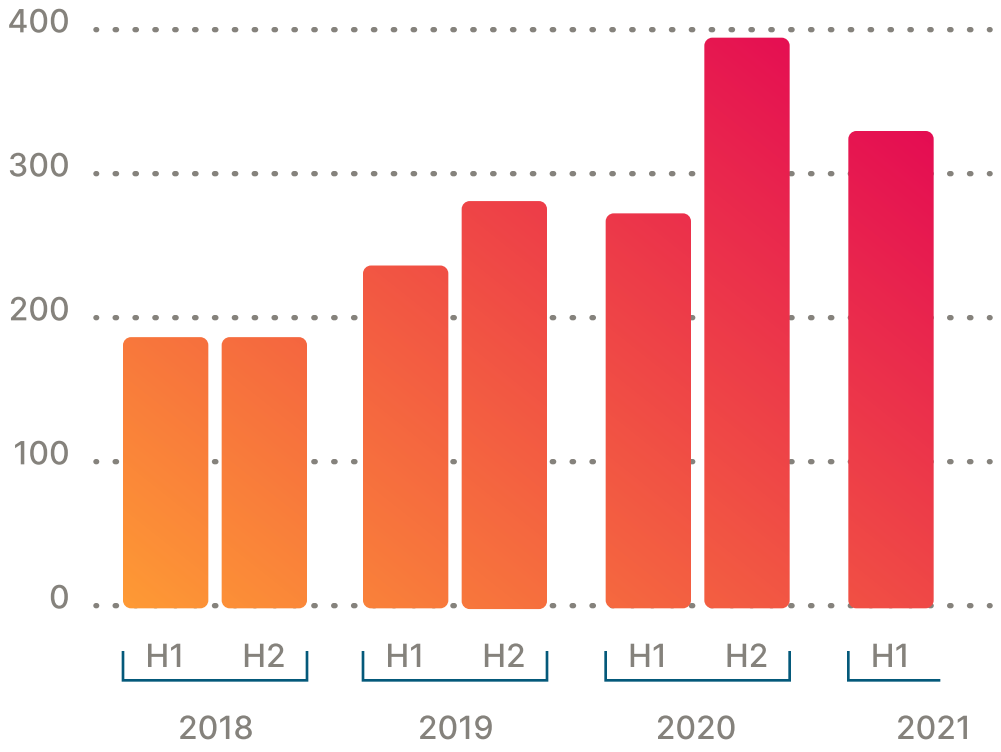
Looking at the U.S. Department of Health and Human Services (HHS) data, the need to improve the industry's cybersecurity posture is critical. As of June 30, the number of breaches reported to the agency this year declined from the second half of 2020. But that number alone provides false hope, as there was a late-2020 ballooning in breached

records due to the Blackbaud breach. The overall trend continues to go up, as we will show in this analysis. As you will see, the number of breaches in the beginning of 2021 was still significantly higher than the first half of last year as well as any six-month period between 2018 and the first half of 2020.

The Department of Health and Human Services categorizes incidents into five categories: theft, improper disposal, loss, unauthorized access/disclosure, and hacking/IT incident. Hacking/IT incident captures any breach that's the result of criminal hackers or compromise in cybersecurity systems and is the main cause of breaches. According to HHS data, more than 70% of the breaches reported during the first six months of 2021 were classified as a "hacking/IT incident."

Not only that, but their targets might surprise you. Outpatient facilities, including family medicine and specialty clinics, were a common source of data breaches, and business associates were heavily targeted as well. The price for these security failures is high. According to IBM's Cost of a Data Breach 2021 report, healthcare data breach costs at the organizations they analyzed averaged $9.23 million, a 29.5% increase from their previous report. As the digitization of healthcare records continues, organizations will need to layer cybersecurity best practices on top of an identity-centric security strategy to protect a growing attack surface.

Total Breaches Reported



PERIOD	COUNT
‘18 H1	185
‘18 H2	184
‘19 H1	234
‘19 H2	278
‘20 H1	270
‘20 H2	393
‘21 H1	327

Key Findings

- Breaches up nearly 2x since 2018 and on an increasing trajectory
- Increase in breaches attributed to hacking/IT incidents, with the number of hacking/IT incidents up over 3x since 2018 on an increasing trajectory
- Business Associates now account for 43% of all healthcare breaches, the continuation of a 3-year upward trend
- Outpatient facilities and specialty clinics were breached nearly as much as hospitals in H1 2021

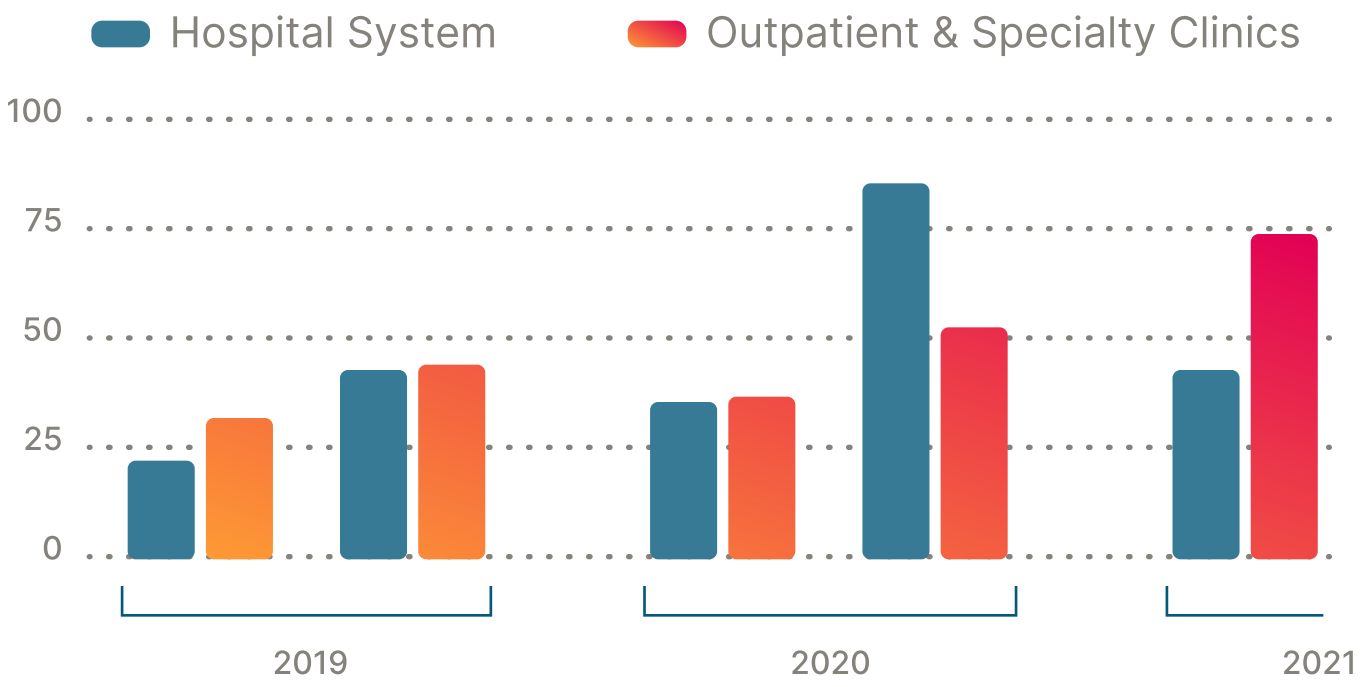
Who is Getting Breached?

Examining breaches caused by hacking reveals something unexpected—attackers hacked outpatient facilities and specialty clinics nearly as much as hospitals. While it may be tempting to think that clinics do not require the same level of cybersecurity diligence as large healthcare systems, that idea is mistaken. Attackers look for the easiest target; if that target is a mental health clinic, that is what they will go after. Smaller organizations run the same systems and use the same technology as hospital systems, making them potentially just as vulnerable. In addition, they also typically have less money to spend on security. For similar reasons, business associates such as claims processors are also frequent victims of attacks. Though these vendors should be covered by business associate agreements (BAAs) that mandate strong security measures,

hackers continue to exploit security gaps at these businesses as a means to steal sensitive data. For example, the Florida Healthy Kids Corporation disclosed a breach of more than 3-million records through a communications design firm.

In the first six months of the year, 141 breaches reported to HHS involved business associates, compared to just 66 in the second half of 2019. As the data

Hospital, Outpatient & Specialty Clinic Hacking by Half Year

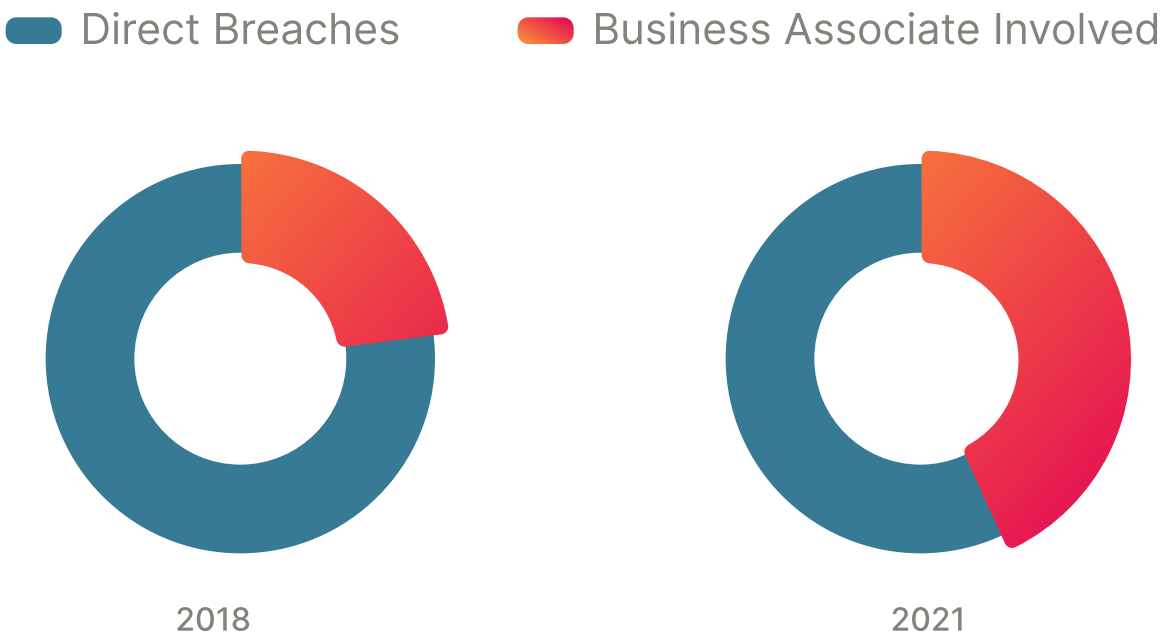


SEGMENT	'19 H1	'19 H2	'20 H1	'20 H2	'21 H1
Hospital System	23	41	31	86	43
Outpatient, Specialty Clinics	34	42	32	51	74

shows, the proportion of business associates impacted by hacking-related breaches has increased with time, standing at roughly half of the breaches reported during the first half of 2021.

The causes of breaches at third-party vendors can run the gamut, ranging from poor access controls that fail to prevent vendors from seeing restricted data to phishing attacks. While business associates have access

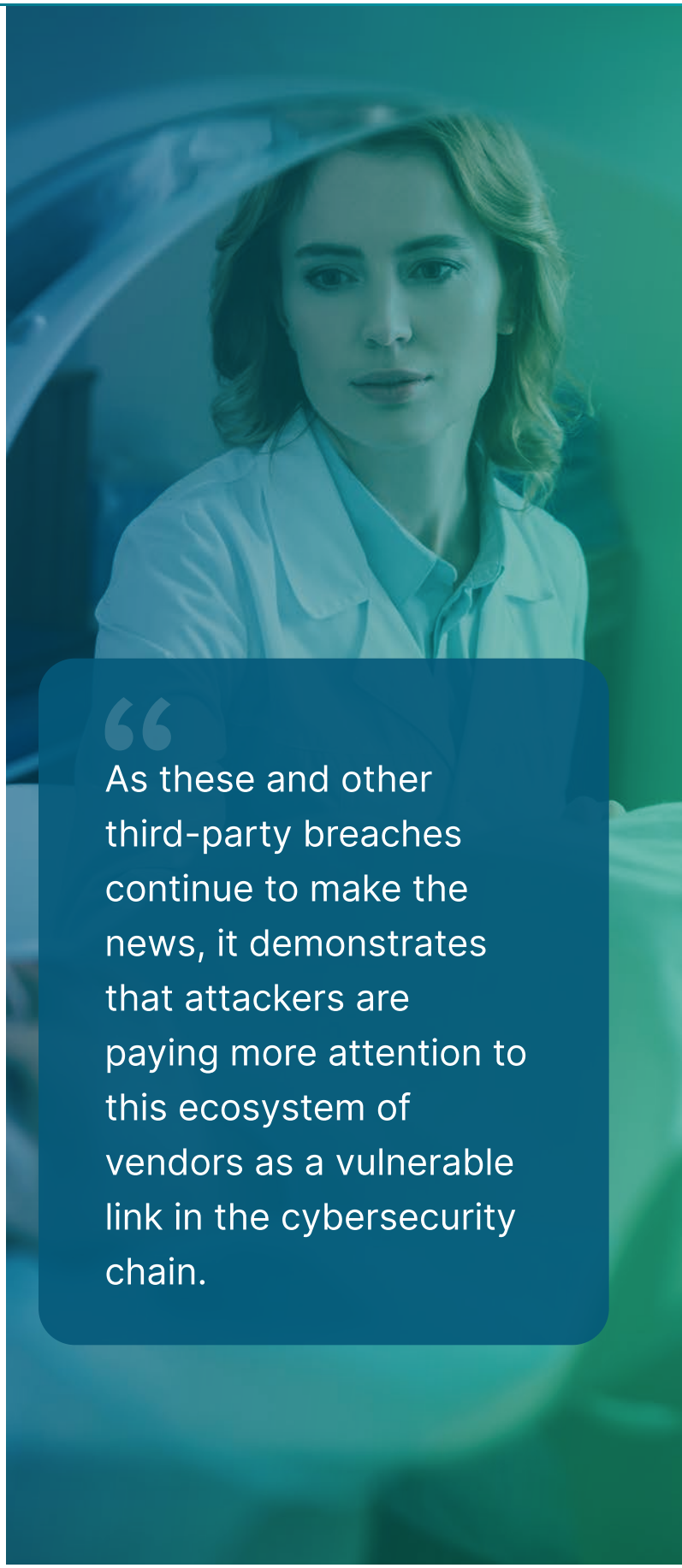
Breaches Involving Business Associates



BUSINESS ASSOCIATES INVOLVED	2018 H1	2021 H1
NO	141	186
YES	44	141

to ePHI, they may not employ the same security standards as their partners. Cloud vendors are not immune. Woodcreek Provider Services reported that a ransomware attack against cloud hosting and managed services provider NetGain Technologies had potentially exposed the records of 207,000 employees, healthcare providers, applicants, contractors, and individuals receiving services delivered by MultiCare Health Systems and Woodcreek Healthcare.

As these and other third-party breaches continue to make the news, it demonstrates that attackers are paying more attention to this ecosystem of vendors as a vulnerable link in the cybersecurity chain.



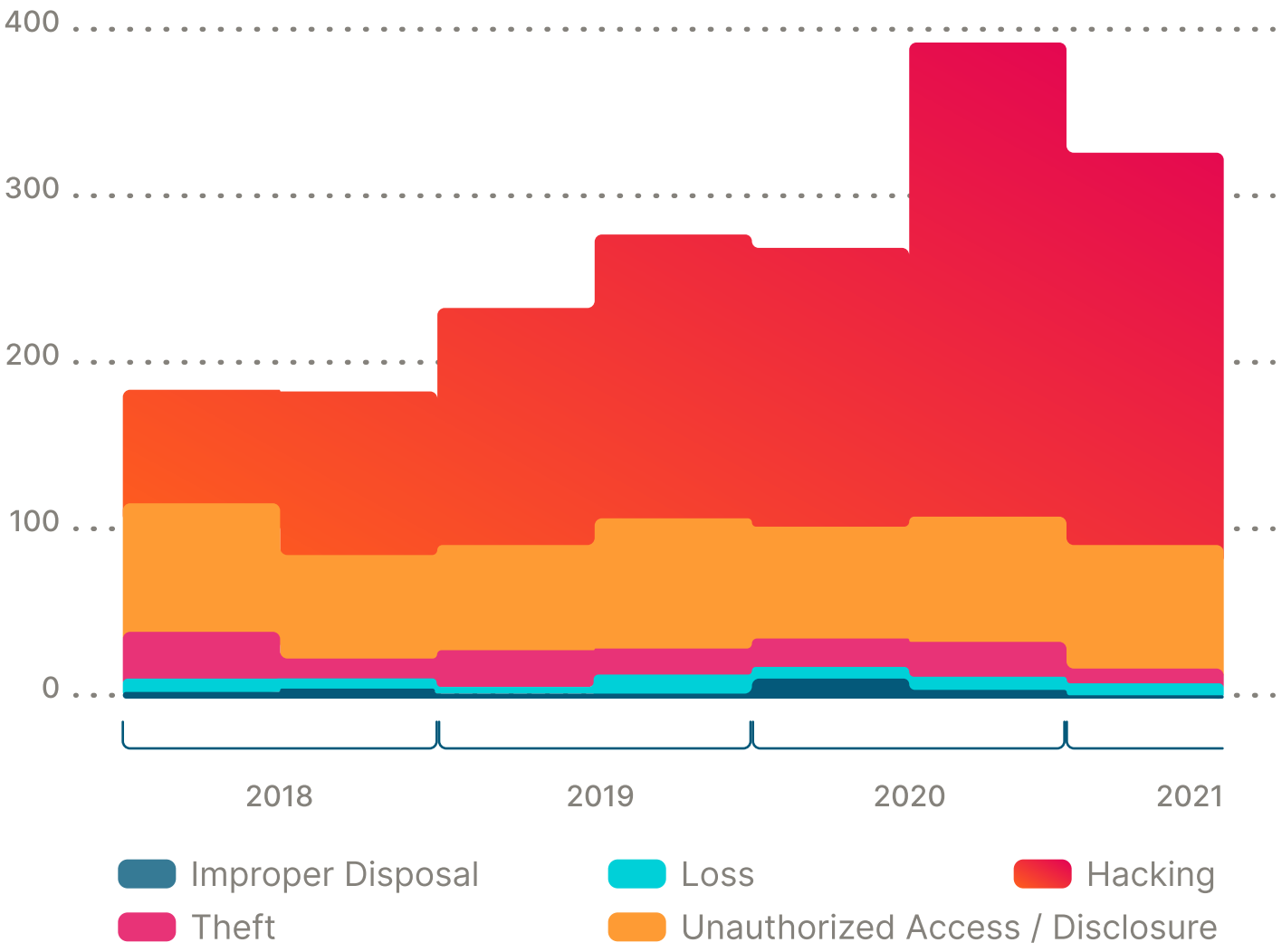
How Are Attackers Targeting the Industry?

Diving down into the data, cyberattacks and IT incidents are the top causes of data breaches, and the main contributor to the increasing number of breaches in the industry. As the diagram on the next page illustrates, the number of data breaches in the first half of 2021 was roughly 77% higher than the number reported to HHS in the first half of 2018. This is mainly due to the increase in hacking/IT incidents, with 235 breaches reported in H1 2021- 3x the number of reports in 2018. The total number of breaches is down from the final six months of 2020, likely due in part to the large number of records breached in the Blackbaud attack last year. But when you go back and look at data from the past three years, the upward trend is clear.

It is no secret as to why hackers are showing interest. Electronic-protected health information (ePHI) is worth more than a credit card number or social security number. Scammers can monetize it in a myriad of ways, from selling it on the dark web to filing fraudulent insurance claims.

It does not help that many health organizations use devices that run on operating systems that are out-of-date, and many devices were not designed with cybersecurity in mind. However, in an environment that prizes performance and constant availability, replacing these devices is neither convenient nor cheap. The interconnectedness of medical devices creates the potential for a catastrophic security failure.

Breaches by Type of Attack



TYPE OF BREACH	'18 H1	'18 H2	'19 H1	'19 H2	'20 H1	'20 H2	'21 H1
Hacking	68	98	142	170	167	284	235
Improper Disposal	4	6	3	3	12	4	2
Loss	8	5	4	11	7	8	6
Theft	28	13	22	16	17	22	10
Unauthorized Access	77	62	63	78	67	75	74

Many of the attacks against the healthcare space involve phishing, ransomware, and the exploitation of vulnerable software. In May, the FBI warned that the Conti ransomware had infected more than 290 healthcare organizations within the past year. The Conti threat actors gained access to their victims through malicious links, infected attachments, or stolen Remote Desktop Protocol (RDP) credentials.

Conti also featured prominently in a June report from the HHS Health Sector Cybersecurity Coordination Center (HC3), which noted that as of May 25, Conti was among the most prevalent ransomware variants it had observed in attacks against the healthcare and public health sector this year. Unfortunately, ransomware attacks are likely to continue as criminals know that the threat of any disruption to the operations of a healthcare organization can provide a strong motivation for the victim to pay.

Email attacks are also one common attack vector cited in the breach data from HHS for the first half of the year. A phishing attack on Saint Alphonsus Health System in Boise, Idaho, earlier this year, for example, impacted more than 134,000 people. In another case, SalusCare, a provider of mental health services located in Fort Myers, Florida, was hit by a phishing attack in March that led to data theft. Given the ease of launching attacks via email, organizations should expect threat actors to continue to use it as a common attack vector in the future.

What You Can Do

In the face of ransomware, third-party breaches, and phishing, healthcare organizations have their hands full. The adoption of mobile devices and cloud computing will also continue to bring their own set of security challenges as well, as healthcare organizations strive to maintain visibility and consistent enforcement of security policies while embracing mobility and a hybrid IT environment. The healthcare industry is a target-rich crucible of remote workers, medical devices running outdated software, and third-party vendors with access to sensitive information. Managing risk in an era of digital transformation comes with a mandate to review their security policies and controls and adjust to a complex threat landscape. For organizations to fight back, they will need to prioritize several key areas.

Assess Third-Party Risk

The abundance of third-party breaches clearly demonstrates that the industry is failing to protect a critical weak point. It is critical for healthcare organizations to classify their business associates by risk level according to the type of data they can access. To develop a third-party risk management program, start by establishing procedures and clear lines of ownership of the processes around vetting third parties. After determining your organization's risk appetite and risk criteria, all vendors should be assessed and then inventoried accordingly. Prioritize reviewing the vendors with the highest risk scores and remediating issues. If you are a third-party, prepare for organizations to ask to see your security papers, such as a recent penetration test or SOC2 Audit.

"The abundance of third-party breaches clearly demonstrates that the industry is failing to protect a critical weak point."

Handling BA Agreements

All business associate aggements should be regularly reviewed. While certain details of BAAs are negotiable, BAAs should include details like what the vendor can or cannot do with ePHI and the duty to report any breaches to the Covered Entity. It is also a good idea for the agreement to contain an indemnification clause and the right for the Covered Entity to audit the vendor's compliance. The number of BAA agreements an organization has can be significant, reaching into the thousands in some cases.

As a result, organizations' knowledge of the existence and the details of BAAs may be fragmented. Organizations need to keep track of the BAAs that are in existence, determine which may have expired, and identify any vendor relationships that should be governed by BAAs but are not.

Ransomware Prevention and Response

Combating ransomware takes a multi-pronged approach. Many ransomware attacks begin with malicious emails containing malware or links to rogue or compromised sites the victim is enticed to visit. Healthcare employees should be trained to be cautious and treat emailed links with suspicion. Beyond this human firewall should be a layer of security provided by a combination of endpoint and network security solutions, that include 24×7 detection and response, a function that can be outsourced to providers like Critical Insight. Additionally, organizations should rely on network segmentation and the principle of least privilege to reduce the ability of the malware to spread. As a final step, organizations should review and periodically test their backup and recovery plans. Organizations with the Critical Insight Total Security Suite have the advantage of Incident Response Planning, advice on backups, 24×7 monitoring, and Incident Response assistance.

Implement Strong Access

Controls Credential theft remains a frequent part of successful cyberattacks and is one of the reasons Zero Trust architectures are discussed so often in the

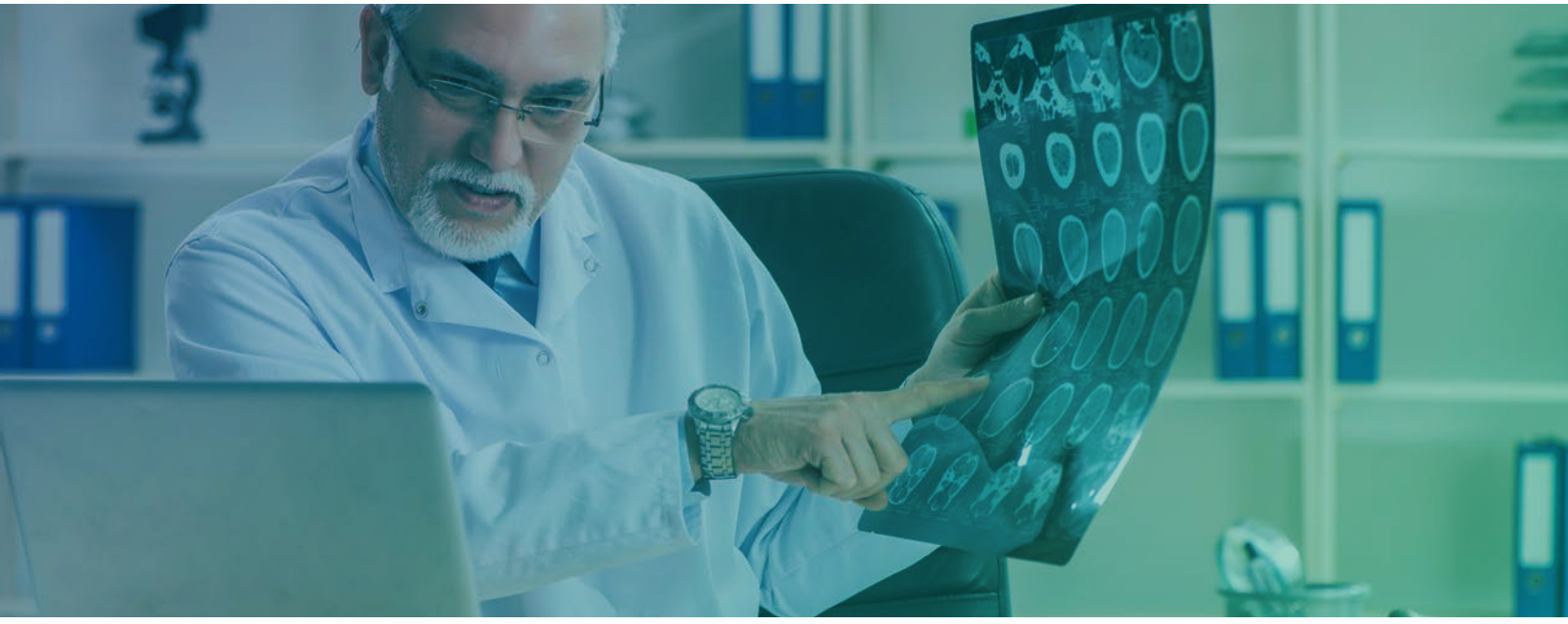
industry. By enforcing strict access controls and segmenting networks, organizations can reduce the effectiveness of phishing attacks and the ability of attackers to move laterally. Identity and access management policies should be built around the principle of least privilege, and enforcing strict access controls is vital for organizations supporting remote workers and using cloud services. For hybrid environments, user and device identity serve as the new perimeter. In the face of this reality, IT leaders are advised to focus on identity and access management as a foundational part of their security strategy. Both healthcare organizations and their business associates should prioritize implementing multi factor authentication and a Zero Trust model if they have not already done so.

Practice Basic Security Hygiene

Zero-day vulnerabilities are not the only way attackers make their way inside healthcare organizations. Unpatched systems and devices that are running software that has reached its end of life present open holes for threat actors. All organizations should prioritize vulnerability management and work to replace legacy assets that are no longer supported. Closing security holes can also be accomplished through security awareness training. Employees that can recognize the obvious signs of phishing will reduce the risk profile of the organization significantly. Careful attention should be taken toward user provisioning and deprovisioning, password management, and the use of data encryption where appropriate. Critical Insight provides a Vulnerability Scanning service that can be integrated with 24×7 monitoring. Additionally, Critical Insight provides free Security Awareness Training.

A Challenging Prognosis

Healthcare professionals are in a challenging time with two massive impediments to patient care: COVID-19 and cybercrime. Those professionals are running organizations that exist in a complex, heavily regulated IT environment that features vulnerable third-party vendors, mobile devices, and all the challenges that come with mixing a hybrid workforce with hybrid IT. All of it has to be secured and managed while threat actors launch attacks against any weak point they can find in the targeted infrastructure. Our analysis of the HHS data reveals that healthcare organizations must focus on a holistic approach to cybersecurity that combines third-party risk management, regular security and compliance assessments, incident response, and 24×7×365 detection and response to ensure patient data is defended.



Disclaimer

This report is for information purposes only. At the time of publication, all information referenced in this report is current and accurate, based on data from the U.S. Department of Health and Human Services Office of Civil Rights Breach Portal ("Wall of Shame") on June 30, 2021. This report may be changed, improved, or updated without notice. Critical Insight is not responsible for any errors or omissions in the content of this report or for damages arising from the use of this report under any circumstances. Major data breaches which affect the unsecured protected health information (PHI) of 500 or more individuals are required to be reported to HHS within 60 days of the discovery of the breach, as required by section 13402(e)(4) of the HITECH Act.

Reporting parameters: Critical Insight analysts reviewed Breach Portal data from the last 36 months, focusing on six-month periods:

- 2018 First-half of the year (2018 H1)
- 2018 Second-half of the year (2018 H2)
- 2019 First-half of the year (2019 H1)
- 2019 Second-half of the year (2019 H2)
- 2020 First-half of the year (2020 H1)
- 2020 Second-half of the year (2020 H2)
- 2021 First-half of the year (2021 H1)

HHS Breach Portal Overview

("Wall-of-Shame 101")

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of 2009's American Recovery and Reinvestment Act, required covered entities and business associates (under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to provide notifications to Health and Human Services about all breaches of unsecured protected health information (PHI). The Breach Notification Rule requires reporting of breaches within 60 days of discovery (in addition to other requirements, but we focus only on reporting in this report). All breaches of more than 500 or more individuals are reported via the HHS Breach Portal. Breaches of less than 500 individuals can be reported to HHS on an annual basis; those reports are not shown in the HHS Breach Portal. The Office of Civil Rights (OCR – the office within HHS that is responsible for administering and enforcing the HIPAA Privacy, Security, and Breach Notification Rules) undertakes investigation and enforcement actions with respect to the reported breaches. The HITECH Act requires that HHS report to several Senate Committees, on an annual basis, a summary of reported breaches, and the actions taken with respect to those breaches.

The latest report available is for 2015/2016/2017. Breach Reports,

submitted through the HHS Breach Portal site, contain several data elements, and these elements were the primary sources used for the generation of this report:

Type of Breach:

- Hacking/IT Incident
- Unauthorized Access/Disclosure
- Theft
- Loss
- Improper Disposal

Types of Covered Entity:

- Health Plan
- Healthcare Clearinghouse
- Healthcare Provider

Business Associate

Location of Breach:

- Desktop Computer
- Electronic Medical Record
- Email
- Laptop
- Network server
- Other portable electronic device
- Paper/Films
- Other

Contributors

John Delano, Critical Insight's Healthcare Strategist
Vivian Zhou, Critical Insight's Healthcare Program Manager

Healthcare organizations looking to improve their security programs work with Critical Insight. The Critical Insight Security Program gives hospitals, clinics, and life sciences organizations an integrated group of services to protect and defend themselves against cyber-criminals. Organizations looking for enterprise-level security programs on a small/mid-market budget turn to CI for its affordability.

CI is a mission-focused cybersecurity company providing Managed Detection and Response and healthcare consulting services.

We protect and defend life-saving, life-sustaining organizations 24/7/365.

Sources

Cost of a Data Breach 2021, IBM, https://www.ibm.com/security/data-breach.

Public Notice of Cyber-Attack Affecting Woodcreek Provider Services, LLC., March 9, 2021, https://www.prnewswire.com/news-releases/public-notice-of-cyber-attack-affecting-woodcreek-provider-services-llc-301243360.html

FBI: Conti Ransomware Actors Exploit Healthcare, First Responder Networks, May 24, 2021, https://healthitsecurity.com/news/fbi-conti-ransomware-actors-exploit-healthcare-first-responder-networks

Ransomware Trends 2021, June 3, 2021, U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3), https://www.hhs.gov/sites/default/files/ransomware-trends-2021.pdf.

SalusCare experiences cyber attack on patient, employee data, March 25, 2021, https://nbc-2.com/news/2021/03/24/saluscare-experiences-cyber-attack-on-patient-employee-data/.

Saint Alphonsus Health System Responds to an Email Security Incident, March 4, 2021, https://www.prnewswire.com/news-releases/saint-alphonsus-health-system-responds-to-an-email-security-incident-301240741.html

Langston, Fred. “Recent Spike in Healthcare Breach Reports Due to Blackbaud Ransomware Attack.” Critical Insight, Critical Insight, 6 Mar. 2021, www.criticalinsight.com/resources/news/article/recent-spike-in-healthcare-breach-reports-due-to-blackbaud-ransomware-attack.