SONICWALL

EXECUTIVE BRIEF

The Transformative Challenges and Complexity of Healthcare Cybersecurity

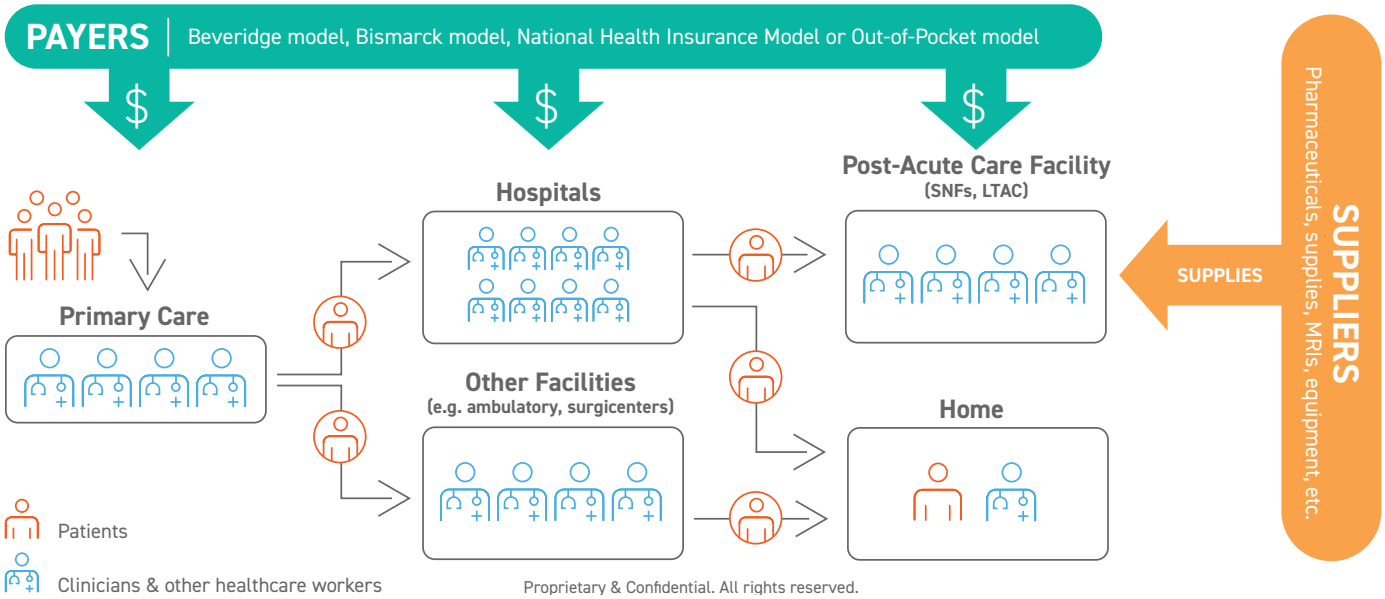
The four critical cybersecurity issues affecting healthcare today.

Abstract

Since the onset of COVID-19, Healthcare Delivery Organizations (HDO) have been shifting and expanding their technology footprints. This growth has been in response to the rapid emergence of telehealth, influxes of remote care professionals, shifts to cloud-based data management and business operations, and proliferation of remote patient-monitoring connected devices. While it's enabled professionals to deliver quality in-person, virtual or at-home care from anywhere, it has also created — or exacerbated — a number of cybersecurity challenges. This brief examines the transformative challenges and complexities of healthcare cybersecurity, which are shared across the global healthcare industry.

Introduction

The stakes are high in healthcare, with new medical technologies and applications affecting the wellness and safety of patients throughout their care continuum journey.



The cascading effects of successful cyberattacks on critical healthcare infrastructures and electronic health records (EHR) can disrupt patient care in some frightening ways:

- Patients don't get the care they need when healthcare providers are taken offline due to ransomware or DDoS attack.
- Surgeons postpone surgeries because the information necessary to perform a life-saving surgery becomes inaccessible.
- Failures in diagnostic procedures and laboratory tests result in delayed medical treatment.
- Emergency Room (ER) bypass causes ambulances to diverge to healthcare facilities miles farther, leading to degraded and irreversible outcomes.

PHI is more valuable on the dark web

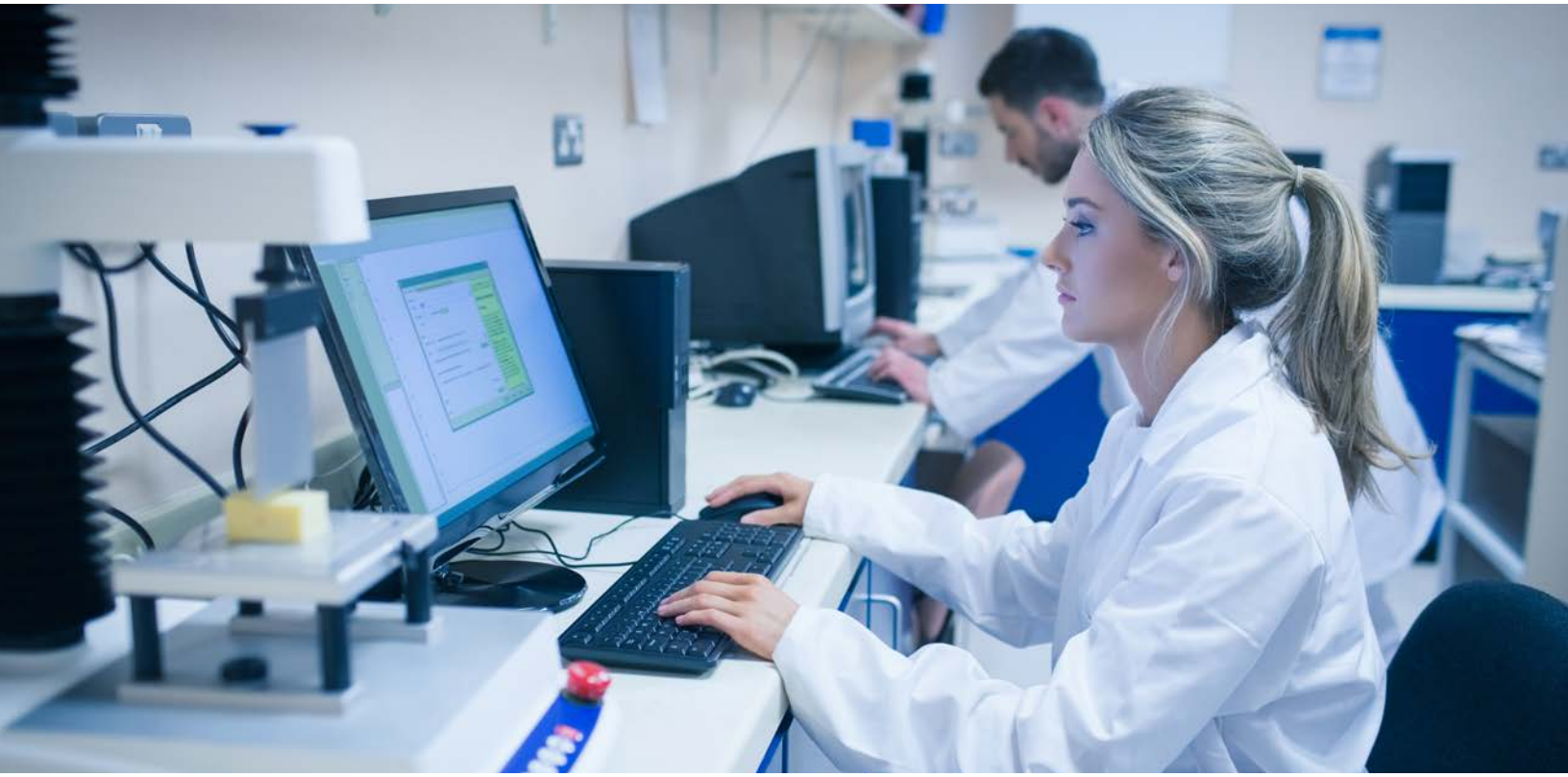
Hospitals and other HDO remain some of the most sought-after targets for external and internal cyberattacks, as protected health information (PHI) is in high demand on the dark web. As a result, PHI can often sell at higher prices than other personal identifiable information (PII).

For example, stolen credit card numbers are deactivated and replaced once suspicious charges are detected, resulting in lower market value. In contrast, medical records have higher valuations because they are immutable data sets that cannot be modified or erased easily. Thus, cybercriminals can continuously benefit, while affected patients suffer financially and emotionally and must take the time to repair damages from fraudulent activities. Some examples include purchasing prescriptions, receiving treatment, filing fake medical claims, or getting personal loans or credit cards using stolen patient health records.

Ransomware troubles persist

Threat actors continue to find ways to exploit weaknesses that healthcare security operating centers (SOC) haven't addressed or noticed because advanced hacking approaches continue to outpace investment in strengthening security controls. For instance, cybercriminals actively go after unpatched vulnerabilities, such as Log4j, as the primary attack vector for launching ransomware attacks. As a result, ransomware is considered the most significant threat across the healthcare industry.

This trend will likely continue through 2022, as 42%[1] of HDO have experienced ransomware attacks in the last two years. In addition, about 36%[2] of those incidents happened via third-party, such as the case of highly publicized supply-chain attacks on vulnerable critical infrastructure management software.



Network server vulnerabilities behind most data breach incidents

The industry experienced its worst year for data breaches in 2021, when a record-breaking number of data breaches occurred and PHI records were exposed. For example, the U.S. Office for Civil Rights (OCR) within the Department of Health and Human Services (HSS) reported that over 700 (Figure 1) covered entities were breached, resulting in the theft, loss, or disclosure of over 42 million individual PHI records (Figure 2). Newly reported incidents[3] reveal breaches and vulnerabilities are already off to a sobering start for 2022 (Figure 3).

Figure 1
Healthcare Data Breaches of 500 or More Records

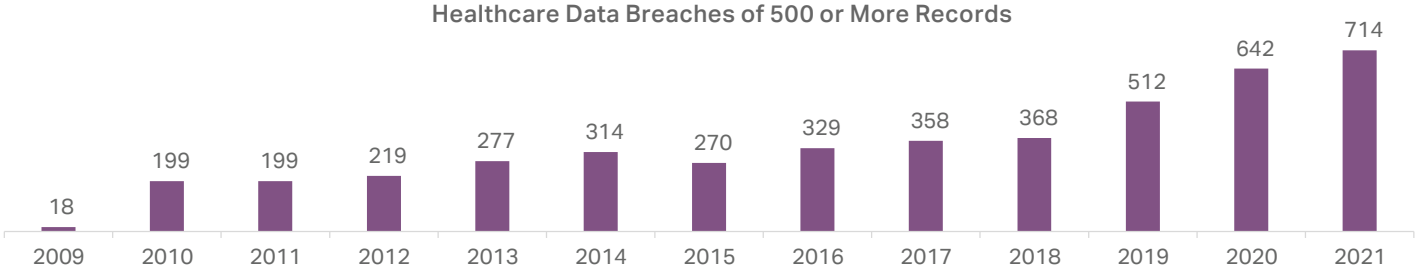
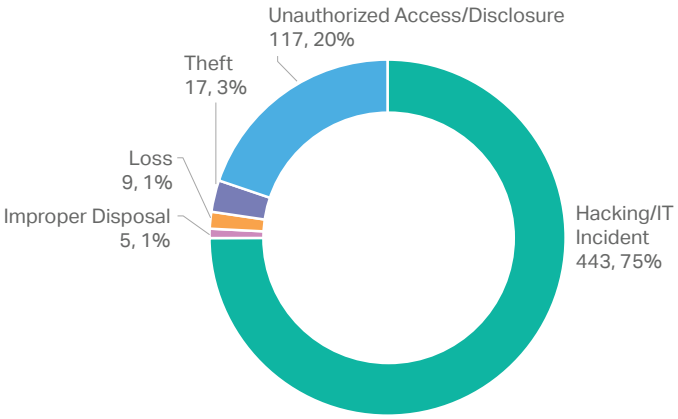


Figure 2

U.S. Department of Health and Human Services Office for Civil Rights, Data Breaches Reported in 2021
Total: 5



U.S. Department of Health and Human Services Office for Civil Rights, Individual Affected in 2021

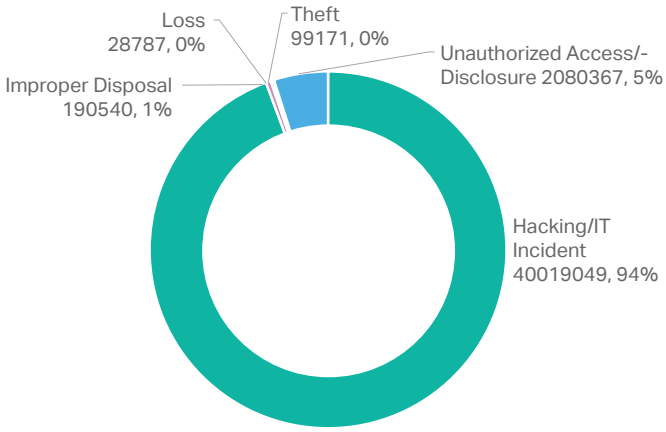
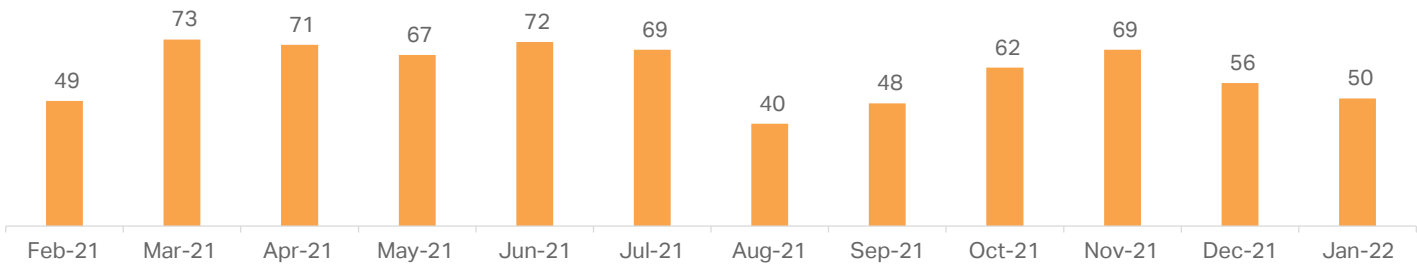
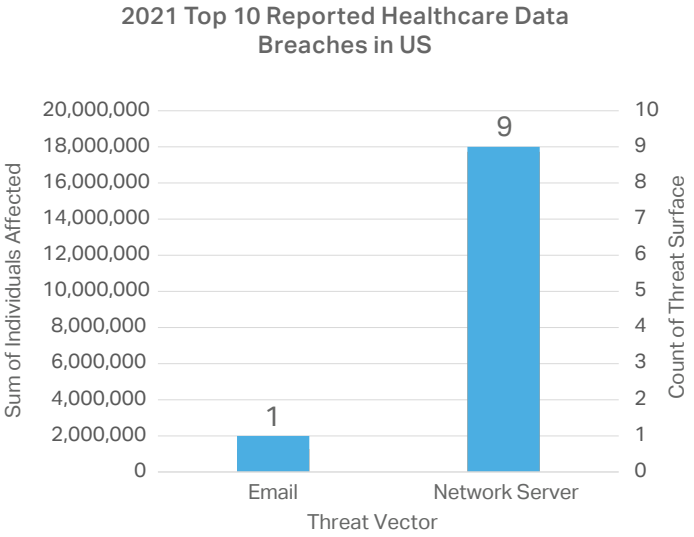


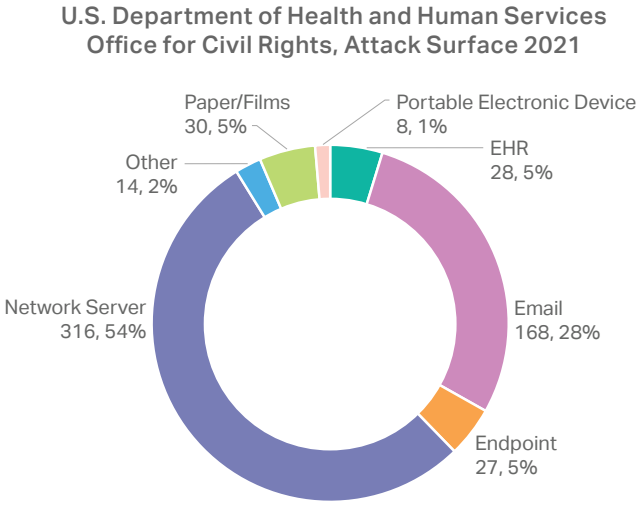
Figure 3
U.S. Healthcare Data Breaches in the Past 12 Months

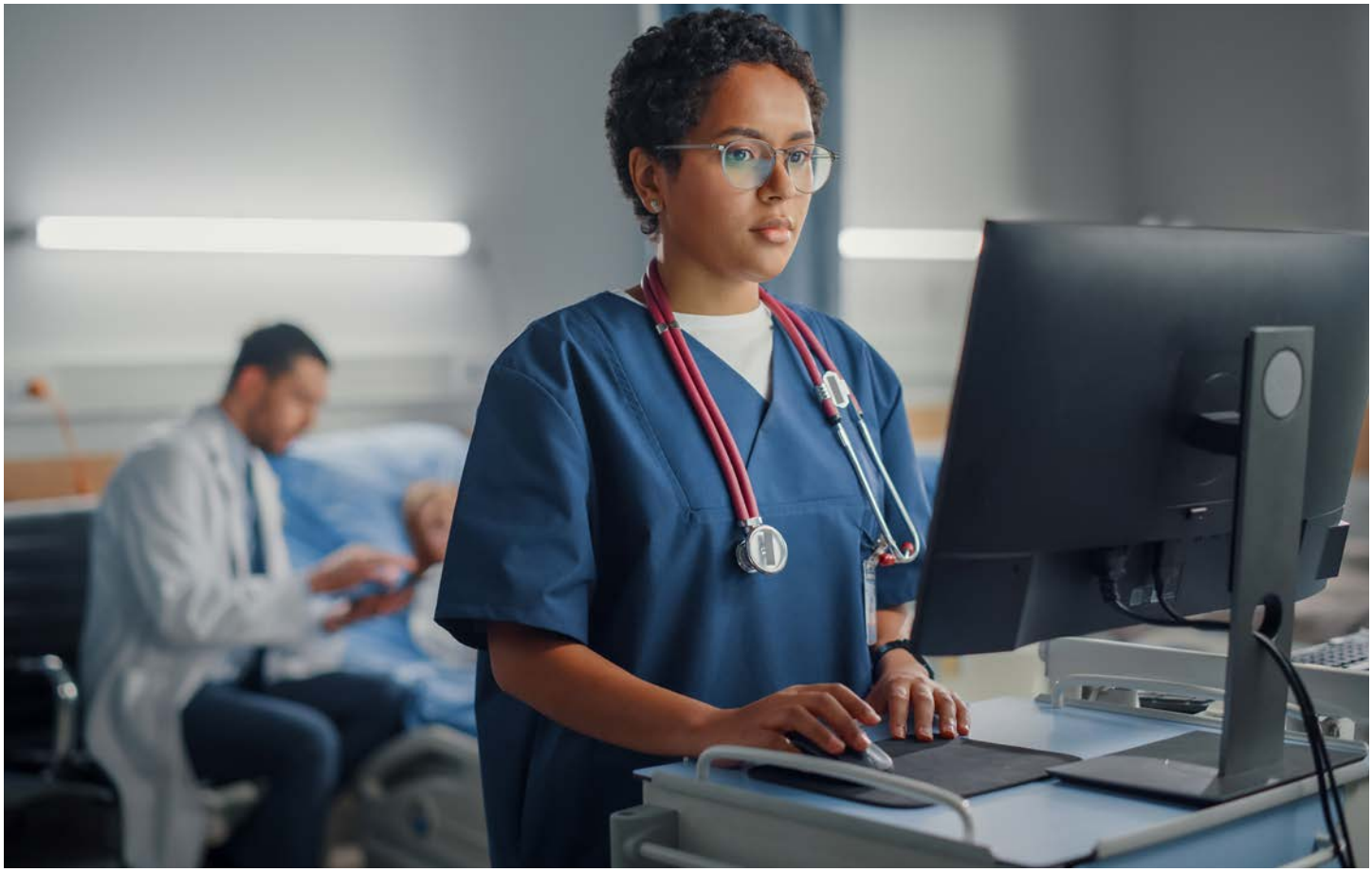


The top ten reported healthcare data breaches of 2021 were all attributed to successful hacking, with severity measured by the number of individuals affected. Ninety percent of those breaches occurred on the provider network servers (Figure 4). Additionally, network server and email combined made up 80% of the attack vectors, adversely impacting acute treatment that could lead to poor outcomes.

Figure 4







SONICWALL®

Four critical cybersecurity risks challenging healthcare

Despite the many benefits technologies bring to healthcare, the adoption of new medical-enabling devices and the interconnection between different healthcare systems adds many risks. HDO face four significant cybersecurity challenges shared across the healthcare industry:

1. Keeping critical infrastructure covered and continuously available
2. Protecting patient privacy from insider risks
3. Preserving the integrity of healthcare data
4. Preventing data breaches originating from ransomware and phishing attacks

Underinvesting in infrastructure security in the context of critical infrastructure expansion creates an untenable situation. Cybersecurity shortcomings in areas such as patch management, configuration management, appropriate access controls, data encryption and patient portal security undermine HDO's mission to deliver quality, timely care and protect patient privacy. Any collapse in the protection of PHI according to applicable data protection laws and guidelines will leave providers at risk for a host of severe consequences. Some examples include data breach, interruption of care, poor treatment outcomes, disruption of billing, financial loss, remediation cost, legal and settlement expenses, heavy fines, erosion of trust, damaged reputation, etc.

Conclusion

While the pandemic persists, HDO remain stretched, understaffed, and overwhelmed with the ongoing healthcare technology and digital transformation to better serve their patients. SonicWall healthcare cybersecurity solution stack is there to help ease the transition and strengthen healthcare infrastructure security, making patient care delivery more efficient, resilient and secure. This integrated, centrally managed security stack consists of edge, data center, access, wireless, email and endpoint, allowing HDO to deliver positive health outcomes for patients throughout their care continuum journey.

Read our Whitepaper "Boundless Cybersecurity for a Safer Healthcare Industry" to learn how SonicWall healthcare-enabling security protects the availability of critical infrastructures, the integrity of electronic health records, and the confidentiality and privacy of personal health information.

1 Source: The Impact of Ransomware on Healthcare During COVID-19 and Beyond by Ponemon Institute.
2 Source: The Impact of Ransomware on Healthcare During COVID-19 and Beyond by Ponemon Institute.
3 Source: HIPAA Journal January 2022 Healthcare Data Breach Report, https://www.hipaajournal.com/january-2022-healthcare-data-breach-report/

About SonicWall

SonicWall delivers Boundless Cybersecurity for the hyper distributed era and a working reality where everyone is remote, mobile, and unsecured. SonicWall closes the cybersecurity business gap for hospitals, clinics and providers worldwide by knowing the unknown, providing real-time visibility, and enabling breakthrough economics. For more information, visit www.sonicwall.com/healthcare.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

SONICWALL®