vertikal 6
TECHNOLOGY. ELEVATED.

A CYBERSECURITY CHECKUP FOR HEALTHCARE

Why small and medium-sized providers are changing how they approach data security.

TABLE OF CONTENTS

GOOD CYBERSECURITY IS GOOD PATIENT CARE

The time has come for small healthcare practices to rethink their approach to cybersecurity. The days of having the jack-of-all-trades "IT guy" handle it with some antivirus software are over. Your "guy" needs backup.

Here's why: Hackers are getting smarter and setting their sights on smaller healthcare practices more than ever before. In just one year, attacks on physician groups jumped from 2% of all healthcare attacks in the first half of 2021 to 12% in the first half of 2022.

Source: Cyber Security Risk Growing for Small Medical Practices, Jan. 17, 2023

And that can have consequences for your business, practitioners, staff – and, yes, patient care.

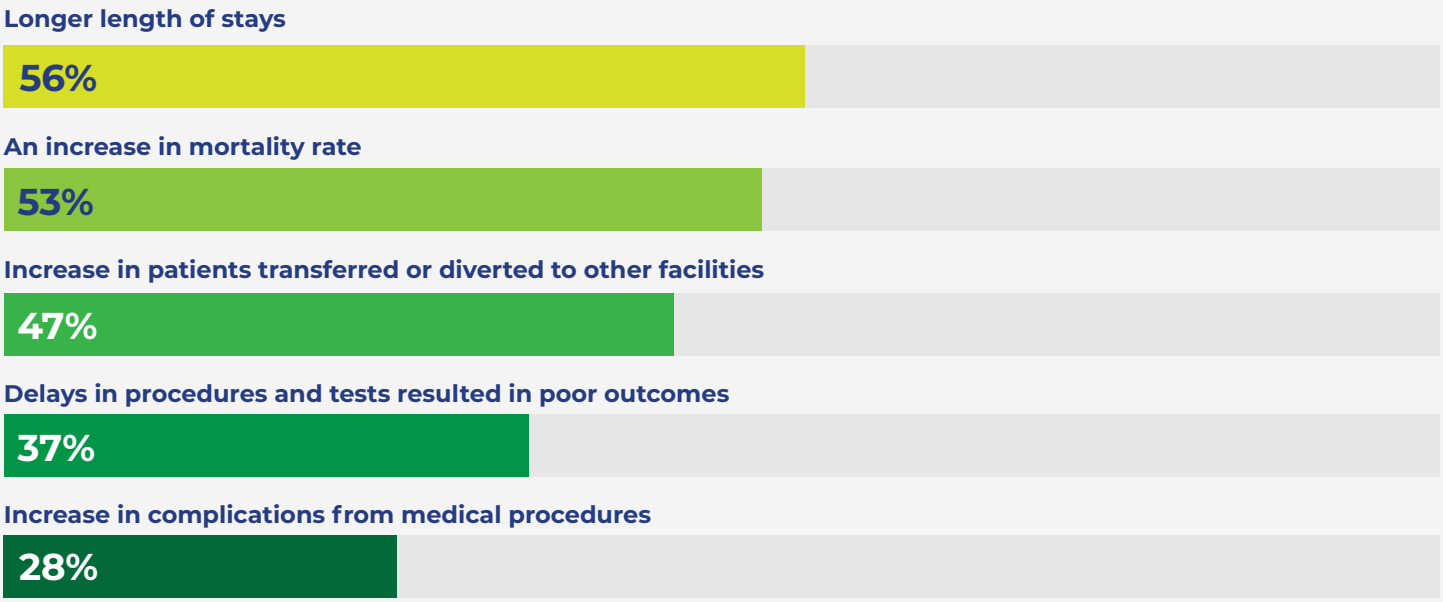
Why Are Criminals Targeting Smaller Practices?

Simply put, they're easier targets. Larger hospitals – once the preferred targets for ransomware, denial of service attacks and other cybercrimes – have been beefing up their security. Hackers are now turning their attention to smaller, less well-fortified operations.

When smaller practices get hit, the fallout can be devastating – imagine for a second the dread that comes with notifying your patients that their personal data has been compromised. Even worse, cybercrime isn't only about harming computers or bottom-line considerations: It has a real-world impact on patient care, slowing reaction time at critical moments. In the words of the American Medical Association, "Cybersecurity is a patient safety issue."

ADVERSE IMPACT OF A CYBERATTACK ON PATIENT CARE ACCORDING TO US HEALTHCARE LEADERS, JUNE 2022

% of respondents



Source: Cynerio and Ponemon Institute, "The Insecurity of Connected Devices in Healthcare 2022," Aug 15, 2022

The good news is that you can better protect your practice and patients by updating how you approach data security.

This e-book delves into the trifecta of modern cybersecurity: Perimeter, Intranet, and Human Security. Through its pages, you'll uncover tailored strategies for each dimension, ensuring your business remains resilient in the face of both current and emerging cyber threats. Arm your organization with the knowledge and tools to build a formidable digital defense.

HEALTHCARE DATA BREACHES IN THE FIRST HALF OF 2023:

327 Data Breaches

104% Increase in Breaches Over the Same Period In 2022

40 Million Patient Records Exposed

Source: "327 healthcare data breaches reported so far in 2023," Becker's Health Care Review, August 10, 2023

BEYOND ANTIVIRUS SOFTWARE & HIPAA COMPLIANCE

It's no secret that the last few years were the perfect storm for medical data vulnerability. An overworked healthcare system faced workforce shortages along with staffing and practitioner burnout, making healthcare a vulnerable target for hackers.

In 2020 alone, 92 ransomware attacks occurred at U.S. healthcare organizations, affecting 600 healthcare facilities and impacting more than 18 million patient records – **a whopping 470% increase from 2019.**

Source: 2020 Offered a 'Perfect Storm' for Cybercriminals," Fierce Healthcare,Mar. 26, 2021

The problem has only increased.

But for small practices, cybersecurity means installing software to detect and eliminate known worms and viruses. Additionally, a HIPAA officer – or, more likely for small practices, the office administrator – oversees regulation implementations. The problem with HIPAA is that it's primarily concerned with patient privacy; it isn't a comprehensive prescription against the various cyberattacks a practice faces. Look at the array of attacks practices face, according to the Healthcare & Public Health Sector Coordinating Council.

MOST COMMON HEALTHCARE CYBERSECURITY THREATS:

- **E-mail phishing attacks**
- **Ransomware attacks**
- **Loss or theft of equipment or data**
- **Insider, accidental, or intentional data loss**
- **Attacks against connected medical devices that may affect patient safety**

Source: Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients

The concerns are growing. With such a complex onslaught, relying on a single defense mechanism is inadequate. And with the advent of generative AI tools like ChatGPT, experts worry there is more chaos in store.

What this means: Small and mid-sized healthcare businesses require a comprehensive suite of cybersecurity solutions to safeguard their operations and data. Broadly outlined, they fall into a few categories: Perimeter Security, Internet Security and Human Security.

THE HIGH COST OF RANSOMWARE:

$11 million – average cost of healthcare attacks in 2023 – a 53% jump from 2020.

Source: https://www.ibm.com/reports/data-breach

Only 64.8% of healthcare data was restored after paying the ransom – only slightly higher than the average of 60.6% across all industry verticals.

Source: https://www.hhs.gov/sites/default/files/2022-retrospective-and-2023-look-ahead.pdf

PERIMETER SECURITY

Establishing A Barrier Between Your Network And The Internet

The advent of web services, cloud technologies, and mobile devices has revolutionized opportunities for healthcare organizations, particularly smaller practices that have struggled to attract and maintain IT staff.

However, it also amplifies the challenges of monitoring the myriad services and solutions in play. A single vulnerability can be the gateway for malware to infest and spread throughout your network.

Addressing such threats necessitates a robust perimeter security framework – a system that regulates access to critical applications, services, and data, denies recognized threats, and monitors suspicious activities. Let's delve into some pivotal perimeter security solutions.

FIREWALLS

Fundamentally, firewalls are a protocol suite determining what traffic is permitted within your network. They scrutinize both inbound and outbound traffic, examining the origin and determining the trustworthiness of payloads.

Historically, firewalls thwarted malware, like Trojans, which aimed to infiltrate networks and pave the way for hackers. Modern firewalls are also adept at preventing unauthorized data transmissions by employees.

INTRUSION PREVENTION SYSTEMS (IPS)

While firewalls are quintessential, they aren't the sole perimeter defense. Their trust-based traffic regulation means crafty hackers can exploit "trusted" sources to bypass them.

Enter the IPS – a system adept at identifying and counteracting malicious network activities. Leveraging "anomaly-based detection," an IPS meticulously examines applications, network packets, IP addresses, and data to detect potential intrusions, even those masquerading as trustworthy. Such detection is instrumental against hackers who subtly modify malware to escape notice. Upon identifying threats, IPSs swiftly isolate or neutralize them, preventing further spread.

36% of cyber-attacks on healthcare organizations were initiated with malicious emails or phishing

SPAM PROTECTION

Email-based attacks (malicious emails or phishing) were the starting points for over a third of attacks (36%) in healthcare organizations.

Source: https://partnernews.sophos.com/en-us/2023/08/resources/the-state-of-ransomware-in-healthcare-2023/

Spam protection tools intercept unsolicited ads and flag emails with dubious attachments, ensuring employees aren't besieged by potentially harmful messages. Sophisticated solutions also feature "safe browsing" capabilities, evaluating the safety of URLs before users click.

However, even fortified perimeter defenses can be breached. Augmenting your system with multiple security layers is imperative to ensure comprehensive protection.

INTRANET SECURITY

While firewalls, Intrusion Prevention Systems, and spam filters shield your network from external threats, they cannot prevent internal vulnerabilities, such as an employee using an infected USB drive. It's analogous to a castle's wall: formidable against external invaders but ineffective once the threat is inside.

Although cybersecurity has modernized significantly since the '80s and '90s, safeguarding individual devices and systems within the local network remains paramount. So how do you reinforce your intranet security?

PATCHING AND SOFTWARE UPDATES

No software is infallible. As technology evolves and new features emerge, vulnerabilities can appear. Vendors frequently release patches to address these weak points. The rapid spread of ransomware like WannaCry underscored the risks of outdated software. Computers with updated Windows versions were immune, spotlighting the importance of timely patching.

ANTI-MALWARE SOFTWARE

The '90s celebrated antivirus software, but today's devices demand comprehensive anti-malware solutions. These programs are equipped with databases of all known threats – viruses, trojans, worms, keyloggers, and more – to shield individual devices from recognized risks. They guard against lingering malware threats, whether from an old USB drive or deceptive emails. However, remember that no solution is foolproof against brand-new malware.

PHYSICAL SECURITY

Amidst the deluge of cyber threats, it's easy to overlook traditional threats like burglary and vandalism. Alongside digital safeguards, it's crucial to integrate physical security, especially for businesses in regulated sectors such as healthcare.

Medical practices have regulations that go beyond just HIPAA, such as Sarbanes-Oxley and PCI DSS, which ensure your defenses are comprehensive, covering both digital and physical protections.

CONTENT FILTERING

A single employee engaging in non-work-related online activities can jeopardize the entire office. From virus-laden ads to phishing links on social media, recreational browsing can be a significant malware source. Implementing a continuously updated content filter minimizes these risks by blocking access to hazardous sites and dubious content.

With a fortified defense against both external cyber-attacks and internal vulnerabilities, there remains one more critical area to address ...

HUMAN SECURITY

High-profile security breaches, often attributed to sophisticated malware or adept hackers, dominate headlines. Consequently, many organizations emphasize perimeter and intranet security, inadvertently sidelining one of the most significant vulnerabilities – their own employees.

Insiders play a larger role in cybersecurity breaches than commonly recognized. Verizon's 2023 Data Breach Investigations Report reveals that a staggering 74% of breaches resulted from actions like answering unsolicited emails, using weak passwords, or connecting to unsecured networks.

Firewalls, anti-malware solutions, and spam filters are ill-equipped to combat threats stemming from human errors or negligence.

Fortunately, preventive measures exist.

EMPLOYEE TRAINING

Just as continuing medical education is a requirement that most providers adhere to because of the evolving nature of threats, continuing education on best cybersecurity practices is essential, especially as it relates to threats from:

- **Social Engineering:** Cybercriminals often prey on trust. Equip employees to identify online scams, dubious links, and deceptive file attachments. Instill a culture of skepticism towards unfamiliar online content.
- **Malware Education:** Clarify malware types, their capabilities, and response protocols for potential infections.
- **Public Hotspots:** For remote workers and BYOD policies, underline the risks associated with public Wi-Fi networks – hotbeds for hacker activities.
- **File-sharing:** Breaches often stem from inadvertent file-sharing or leaving sensitive files unattended. Educate staff about sharing permissions and promote a clean-desk policy.

74% of breaches are internal.

PASSWORD POLICIES

Weak passwords remain a recurring chink in cybersecurity armor. Astonishingly, basic passwords like "123456" are still prevalent.

Hackers, employing brute-force attack methods, can effortlessly deduce such passwords. Mandate complex, lengthy, and unique passwords across different accounts, reducing vulnerabilities.

SECURITY TESTING

After training, assess employee application of knowledge through security tests. Use quizzes on phishing, malware, and secure practices.

Role-play scenarios replicate common scams, and hiring penetration testers offers a deeper defense assessment. Regular evaluations, preferably quarterly, refine employees' cybersecurity proficiency.

A holistic security approach integrates Perimeter, Intranet, and Human Security, ensuring comprehensive protection on all fronts.

INTEGRATING ALL APPROACHES: THE ROLE OF THE MSP

Tailoring A 24/7/365 Security Blueprint for Today's Healthcare Practices

Today's multifaceted threats demand more intricate solutions for even small healthcare providers. The pillars of cybersecurity – Perimeter, Intranet, and Human Security – must be customized to your business, factoring in the high-stakes environment.

One solution: Allocate substantial resources to build an expansive IT support team adept at handling daily and long-term regulatory and cybersecurity challenges. But this is likely financially untenable for many small and medium-sized practices.

Enter Managed IT Service Providers (MSPs) – a cost-effective solution offering cybersecurity expertise. For an economical monthly fee, you access a diverse team of IT specialists who can help your office manage the technology it needs to operate efficiently and safely.

Opting for an MSP ensures that someone is addressing every facet of cybersecurity with vast expertise to create a modern, secure environment to guard against days rapidly evolving challenges:

- Prevent downtime or system outages from impacting your practice with 24/7/365 monitoring and IT support.
- Maintain compliance with stringent regulatory requirements such as HIPAA, even while your IT environment and industry evolve.
- Safeguard protected health information (PHI) and the lives it directly impacts.

It's important to remember that cybersecurity isn't a one-time thing; it's ongoing. Just like continuing medical education allows practitioners to stay up-to-date with the latest best practices, working with an MSP allows your organization to stay ahead of the curve as new challenges and opportunities arise.

SECURING YOUR DIGITAL FUTURE

Cyber threats are continually evolving, demanding more than just isolated security measures. As we've explored in this e-book, modern businesses must integrate ...

Perimeter security

Intranet security

Human security

Today's practices – whether solo practitioners or multi-office regional medical groups- must tailor strategies to their unique needs to ensure an effective defense. Equipping your organization with comprehensive cybersecurity measures is about thwarting external attacks and fostering an informed, vigilant internal culture.

ARMING HEALTHCARE PROVIDERS AGAINST TODAY'S CYBER THREATS

Want to see our approach to healthcare cybersecurity firsthand?

Call us today to talk with one of our seasoned consultants. We're here to address your concerns, offer insights specific to healthcare, and thoroughly audit your existing IT infrastructure.

Together, let's fortify your healthcare organization against the cyber challenges of tomorrow.

REQUEST YOUR FREE CONSULTATION TODAY!

401-825-4401 INFO@VERTIKAL6.COM WWW.VERTIKAL6.COM/

vertikal 6
TECHNOLOGY. ELEVATED.