MEDITAB™
INTELLIGENT MEDICAL SOFTWARE

CYBERSECURITY STRATEGIES

A Guide For Small Medical Practices

A Meditab Software Inc. White Paper

TABLE OF CONTENTS

Introduction:

HEALTHCARE IS UNDER ATTACK

CYBER ATTACKS ON BUSINESSES AND CRITICAL INFRASTRUCTURE ARE INCREASING.

From 2020 to 2022 alone, cybercriminals have doubled the frequency of attacks while concentrating their efforts on healthcare providers.

The healthcare industry isn't just an attractive target; it consistently ranks among the top victims of cybercrime and experiences the most expensive[1] data breach costs. With access to names, addresses, credit cards, and social security numbers, healthcare systems possess a treasure trove of valuable data ripe for the taking.

You may think small practices like yours are safe amidst bigger targets like hospitals and health centers; in reality, small health clinics are prime targets for cybercriminals. This false sense of security puts small practices in danger through relaxed security measures and unguarded endpoints. Practices that don't see themselves as potential victims are less likely to be prepared for an attack or devote enough resources towards cybersecurity until criminals strike.

Unfortunately, the time to take action is before an attack, not after. Once your accounts are compromised, or your software is infected with ransomware, it's often too late to stop the damage. Staying complacent and failing to take the proper steps today may cost your practice time, money, and reputation tomorrow.

This whitepaper will explore how cybercriminals exploit vulnerabilities to cause severe financial damage and explain what steps small medical practices like yours should take to prevent attacks. With effective cybersecurity strategies, your practice can thwart attackers and preserve the integrity of your sensitive data.

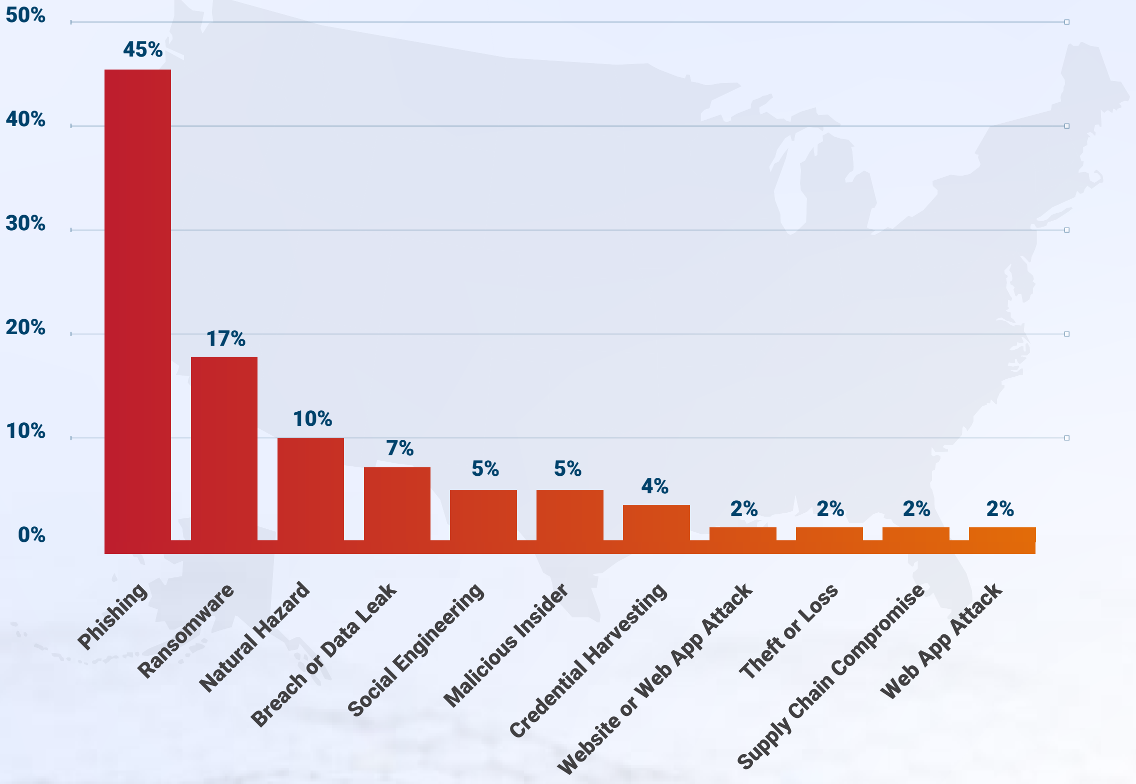
The Anatomy of a Cyber Attack:

HOW CYBERCRIMINALS THREATEN YOUR PRACTICE

CYBERCRIMINALS USE VARIOUS METHODS TO ATTACK SMALL MEDICAL PRACTICES,

including phishing scams, ransomware, data leaks, distributed denial of service (DDoS) attacks, and more. **Understanding the differences between these attack vectors will help your IT team identify threats and prevent breaches to your network.**

Cyber Security Incidents in US Healthcare Organizations[2]



Cyber Attack Vectors

Ransomware is among the most devastating forms of cyber attacks.[3] Ransomware encrypts your files, making them completely inaccessible. Criminals then charge your practice a massive sum to unlock the files, crippling your practice and putting your patients' health in jeopardy.

"In my experience, a large number of practices are not equipped to deal with ransomware attacks and lack the knowledge to respond effectively," **says cloud computing expert Wayne Larsen of industry-leading IT firm ER Tech Pros.** *"The aftermath of a ransomware attack can be catastrophic, causing extensive disruption to business operations, loss of vital data, and irreparable harm to the organization's reputation."*

Sadly, paying ransomware fees can be less expensive than rebuilding new IT infrastructure from scratch and struggling through weeks of downtime. Cybercriminals use this to their advantage to coerce practices into paying up, often under the pressure of deleting invaluable medical records.

However, ransomware doesn't just target a practice's financial stability and ability to operate—it also risks the safety of patients' lives by compromising confidential information, which can include social security numbers, addresses, and credit cards.

The Healthcare and Public Health Sector is the number one[4] ransomware target and experiences up to 25% of all attacks.

"In several cases," **continued Mr. Larsen**, *"I have witnessed cybercriminals manipulate the situation by forcing organizations to pay ransom under the pressure of exposing sensitive medical data."*

Diaxin Ransomware: #StopRansomware

In October 2022, the F.B.I., Cybersecurity and Infrastructure Security Agency, and Department of Health and Human Services continued their joint initiative called #StopRansomware in response to devastating ransomware attacks from Team Diaxin—a cybercriminal organization. The attackers have targeted the Healthcare and Public Health Sector through unprotected Virtual Private Networks (VPN) and caused millions of dollars in damages by encrypting their files.

The lesson for practices like yours:
ransomware threats are evolving; only the most prepared organizations can keep up.

Phishing - Unlike a traditional computer virus that steals information by infecting a system, phishing criminals trick people into giving over personal information. To get credentials, phishing scammers fake their identities to lower a victim's defenses. This disguise often appears as a spoofed email address, phone number, or physical mail that mimics the identity of someone you trust. Accompanied by a sense of urgency, it's easy to fall victim to a professional phishing attack.

PHISHING

QUICK TIPS

1. Check embedded links before clicking.
2. Look for suspicious "From:" addresses.
3. Be cautious with "urgent" or "too good to be true" messages.

2022 Data Breach Costs:[6]

$4,350,000

AVERAGE TOTAL COST

$164

PER RECORD

DDoS (Distributed Denial of Service) attacks are a type of cybersecurity threat designed to disrupt the operation of websites and services by flooding them with requests.

When under attack, a massive amount of malicious traffic is sent to overwhelm a website's servers, rendering them inaccessible to their intended users. Malicious parties use these attacks to spread propaganda or deny access to important data and information.

DDoS prevention is an integral part of any organization's cybersecurity strategy, and security specialists must stay up-to-date on the latest DDoS attack vectors to mitigate this risk.

Cyber Vulnerabilities

It's essential to consider what vulnerabilities your practice's IT system may have. While you can't control the actions of malicious criminals, understanding your hardware, software, and user limitations will allow you to make the changes necessary for a strong cyber defense.

Compromised Credentials are a significant concern in cybersecurity, as they allow attackers to bypass traditional authentication measures and gain direct access to user accounts. This can have serious repercussions, including the potential for malicious actors to take over users' identities, steal sensitive information, or open the door to other types of malware and phishing campaigns. Practices should reduce exposure risks by practicing good password hygiene, using multi-factor authentication, and screening for compromised credentials.

It takes an average of **243 days** to identify compromised credentials and an additional **84 days** to contain the breach.[7]

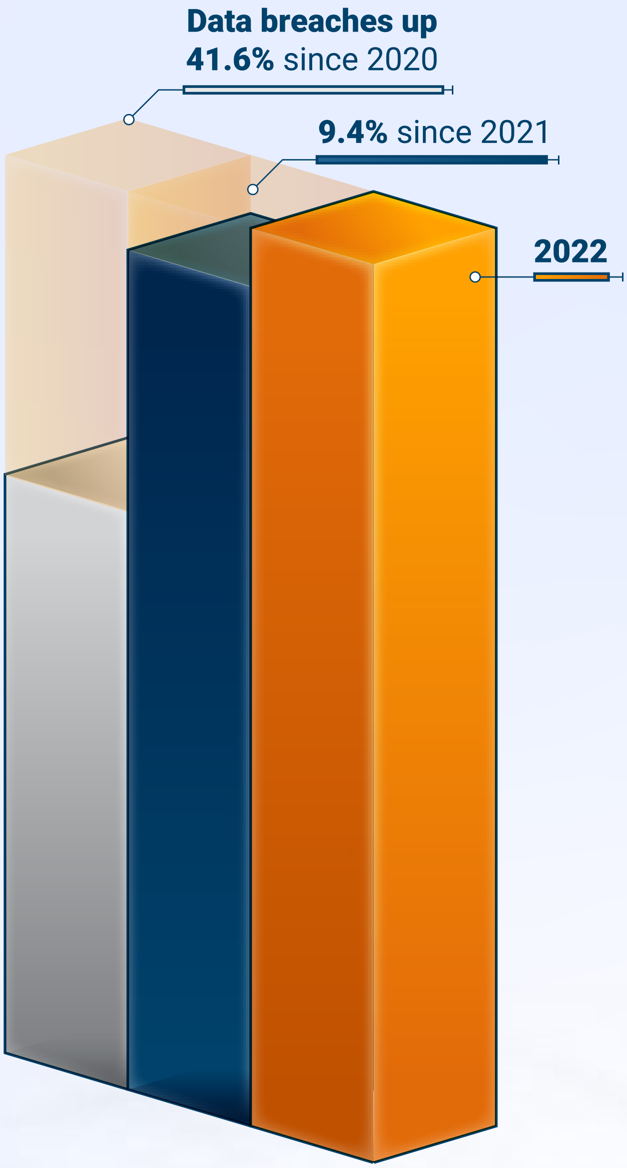
3rd-Party Software Vulnerabilities - Your defense network is only as strong as its weakest link. For practices with strong cybersecurity defenses, cybersecurity openings are often found through a third-party software provider who doesn't take security seriously. Your organization may be unaware of these vulnerabilities, but by allowing their software into your network, you'll create opportunities for cybercriminals to access your systems.

Legacy Systems -The older our systems get, the more likely they become compromised. Legacy hardware and software systems tend to lose developer support after five years, which makes them more vulnerable as time goes on.

Compliance Failures - Practices often lack the knowledge and guidance to create a secure environment that protects confidential information and data. And even if the correct guidelines are in place, that doesn't mean every employee is sufficiently trained to follow them.

When your team lacks standard cybersecurity procedures or sufficient training, compliance failures can lead to costly sanctions or disruptions in operations if a breach occurs. It only takes one slip-up to create an emergency!

Healthcare Breaches Hit Record High[8]



CYBER DEFENSE SOLUTIONS FOR SMALL MEDICAL PRACTICES

A strong cyber defense begins with the right strategies. The best approaches involve multi-layered defenses that cover all potential avenues of attack.

Besides technology solutions that thwart attacks, you'll also need to consider resources to deploy in the unfortunate scenario of a data breach. The longer it takes to detect and respond to a cybersecurity breach, the more costly it will be. By deploying a proactive cybersecurity initiative, your practice can see incident response savings of up to 58% and lower detection & response times by 10%.[9]

> *By deploying a proactive cybersecurity initiative, your practice can see incident response savings of up to 58% and lower detection & response times by 10%.*

Cloud Hosting - Cloud server hosting eliminates the biggest immediate threat to data: physical security. Unlike on-premise solutions, cloud servers are much more difficult to access by malicious actors.

You'll also reduce some of your largest IT costs by switching to the cloud. Instead of housing physical servers on-premises, running 24/7 monitoring, and maintaining infrastructure, you can save space, bandwidth, and resources by letting a professional cloud hosting provider handle the logistics for you.

Managed Firewall - Like lanes on a highway, internet ports allow traffic to move through your network. The more pathways open, the more avenues of attack cybercriminals have to breach your systems. A great firewall system manages your network traffic to ensure unused access ports are closed to traffic and only approved traffic gets through to your IT systems. They can also inspect outbound traffic to prevent malicious software from phoning home to command-and-control servers.

Dark Web Monitoring - A Dark Web monitoring service will have a permanent presence on the most common dark web hubs and search for data relevant to your practice. That way, if your data is compromised, your IT team will be alerted immediately to the breach and prevent further damage.

Don't Know Where to Start? Ask the Pros!

Working with a trusted partner like ER Tech Pros can take your cybersecurity defenses to the next level, especially for small medical practices with limited resources. According to Director of Cybersecurity Sumair Sidhu, your #1 priority should be getting critical services like response teams and data recovery in place now to limit potential damage later. *"By taking proactive steps and putting yourself in a position to act fast, my team can identify, quarantine, and eliminate threats to protect the integrity of our partners' data, even in worst-case scenarios."*

Multi-Factor Authentication - Multi-factor authentication (MFA) provides an additional layer of protection for accounts, making it much more difficult for hackers to access or delete sensitive data. With MFA, users will need to confirm their identities through verified channels—like verification codes, fingerprints, or face scans—before successfully logging in. This serves as an effective line of defense against cyberattacks and other malicious activities, helping you secure digital assets

Response Team - Having a dedicated incident response team that can identify, investigate, analyze, and respond to potential threats provides practices with the insights and confidence they need to protect their data. Incident response teams can also develop strategies to prevent similar attacks in the future, ensuring greater security. They are well-positioned to stay up-to-date on industry best practices and new technologies that strengthen cyber defenses, further reducing the risk of a data breach. Don't underestimate invaluable expertise that can't be matched by relying solely on passive security controls.

Recovery and Backups - Keeping confidential data safe is challenging, but a reliable data recovery plan can help. A professional response team is the best way to ensure that any lost or stolen data is efficiently and effectively recovered. By implementing data recovery procedures ahead of time, businesses can rest assured knowing their critical information will remain secure even if something unexpected happens.

AI and Machine Learning - AI and machine learning are increasingly popular features of cybersecurity tools. Backed by powerful AI, machine learning systems actively monitor networks and computer systems and analyze usage patterns to detect suspicious activity. Advanced learning algorithms are trained to recognize events and signs that may indicate a cyber-attack, allowing for more efficient security threat detection. This significantly reduces costs associated with traditional manual cyber defenses by automating procedures, such as policy enforcement, antivirus installation, and patch management.

3 CYBERSECURITY STEPS YOUR PRACTICE CAN TAKE NOW

01

Cyber Readiness Analysis - The first step is evaluating your practice's readiness with a professional Cybersecurity Readiness Assessment. A Cybersecurity Readiness Assessment will test your defense systems by simulating cyber attacks to determine weak points and highlight areas for improvement.

"Too many small practices are failing to take the time to properly review their cybersecurity systems," **says ER Tech Pros CEO Shameer Nalli.** *"Over the years, our cyber readiness analysis team has saved countless businesses by discovering, fixing, and preventing major gaps in their defenses. If you haven't taken the time to test your systems with a professional, there's a strong possibility your practice is open to attack."*

A Cybersecurity Readiness Assessment will review:

Server Hosting Environment

- ☑ How old is your equipment?
- ☑ Do you have EDR?
- ☑ Are servers regularly patched and maintained?

Endpoint & Network Security

- ☑ Do you have a fully deployed endpoint detection and response system?
- ☑ Is your firewall actively managed and maintained?

Data Management

- ☑ Is your data securely backed up?
- ☑ Do you have a disaster recovery server?

In the meantime, users can employ common sense tactics to reduce the risk of cyber-attacks and limit potential damage.

Common Sense Cybersecurity Checklist: Protect Your Practice

- Create Strong Passwords
- Use A Firewall
- Install Anti-Virus and EDR Software
- Practice Safe Browsing Habits
- Control Access to Computers & Networks
- Back Up Your Data

02

Zero Trust, Always Verify - In today's world, "zero trust, always verify" is an essential maxim of the best cybersecurity policies. By assuming nothing and verifying everything, zero trust provides the highest possible level of security against insider threats, data leakage, and unauthorized access to networks. A zero-trust system authorizes each user individually and tracks their activities within the organization's cloud environment or network. This stringent authentication process provides greater protection than traditional cybersecurity practices, such as passwords and firewalls. Zero trust is a must-have cybersecurity practice to ensure unhindered business operations that are secure and compliant.

03 **Cloud or Hybrid Server Implementation** - Cloud and hybrid server hosting offer an excellent security solution for practices of all sizes. By using cloud or hybrid servers, practices can store data with more defense measures in place than they could on their own.

Additionally, cloud hosting provides access to a range of cybersecurity services, such as virus protection, malware shielding, and recurrent backup systems that keep records safe. With this setup, cloud computing technology is combined with the practice's own hardware resources to ensure excellent performance while keeping important assets secure from outside attacks. Together, these cloud hosting solutions protect private information from malicious activity while incorporating the most up-to-date technology into operations.

CONCLUSION

Cybersecurity is a critical issue for small medical practices. They remain especially vulnerable to cyberattacks because they often have limited resources and staff. However, there are steps that small medical practices should take to protect their IT systems.

In this whitepaper, we have outlined several cybersecurity strategies that small medical practices like yours can use to defend themselves. Cybersecurity is a complex issue, but by following the tips in this whitepaper, small medical practices can prevent the devastating effects of a cyberattack.

ABOUT MEDITAB SOFTWARE INC.

With a quarter century in the healthcare technology space,
Meditab Software Inc. is recognized as an established industry leader.

Since 1998, Meditab has helped practices improve workflows, increase cybersecurity, and deliver high-quality care with innovative services and solutions.

www.meditab.com

sales@meditab.com

1-844-4-Meditab

8795 Folsom Blvd., Suite 205,
Sacramento, CA 95826

BEGIN YOUR CYBERSECURITY JOURNEY TODAY

Connect with Meditab Software, Inc.'s cybersecurity experts to learn how your practice can develop a professional cybersecurity defense to protect valuable patient data.

Request a Demo >

REFERENCES

1. **"IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High."** *IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High*, 27 July 2022

https://www.prnewswire.com/news-releases/ibm-report-consumers-pay-the-price-as-data-breach-costs-reach-all-time-high-301592749.html

2. Petrosyan, Ani. *Share of Significant Cyber Security Incidents Experienced in Healthcare Organizations in the United States in 2021. Statista*, Jan. 2022

https://www.statista.com/statistics/1237131/cybersecurity-incidents-in-healthcare-organizations-us/

3. **"Ransomware Activity Targeting the Healthcare and Public Health Sector."** Cybersecurity and Infrastructure Security Agency, Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, Department of Health and Human Services (HHS), 2020

https://www.cisa.gov/uscert/ncas/alerts/aa20-302a

4. Federal Bureau of Investigation Internet Crime Report 2021. Federal Bureau of Investigation , 2022

https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

5. #StopRansomware: Daixin Team, The Federal Bureau of Investigation, The Department of Health and Human Services, The Cybersecurity and Infrastructure Security Agency, Oct. 2022

https://dd80b675424c132b90b3-e48385e382d2e5d17821a5e1d8e4c86b.ssl.cf1.rackcdn.com/external/aa22-294a-stopransomware-daixin-team.pdf

6. **"Cost of a Data Breach Report 2022."** Cost of a Data Breach 2022: A Million-Dollar Race to Detect and Respond, IBM Corporation, July 2022

https://www.ibm.com/downloads/cas/3R8N1DZJ

7 - 9. Ibid.