

HOW TO LOWER **CYBERSECURITY RISKS IN HEALTHCARE**





Healthcare is a prime target for cybercriminals. Protected health information and electronic medical records are a data treasure trove. The threat is real ... and growing. This ebook outlines the cybersecurity risks in healthcare. We also share best practices and benefits of a managed services provider's help.





No wonder adoption could reach 75 billion IoMT devices worldwide by 2025.


The problem is in securing these devices along with existing systems and networks. Healthcare providers store sensitive medical and financial information, and hackers are always developing more ways to gain access to data or hold data and networks for ransom.

The Risks for Healthcare Providers

Let's start with December 2020 examples. GE Healthcare identified two critical vulnerabilities impacting more than 100 of its products. The software vulnerabilities affecting MRI, X-Ray and ultrasound devices allow remote code execution. That allows access or alteration of sensitive patient data.

Also in December:

- Cybersecurity Infrastructure and Security Agency warned of phishing targeting those distributing COVID-19 vaccines.

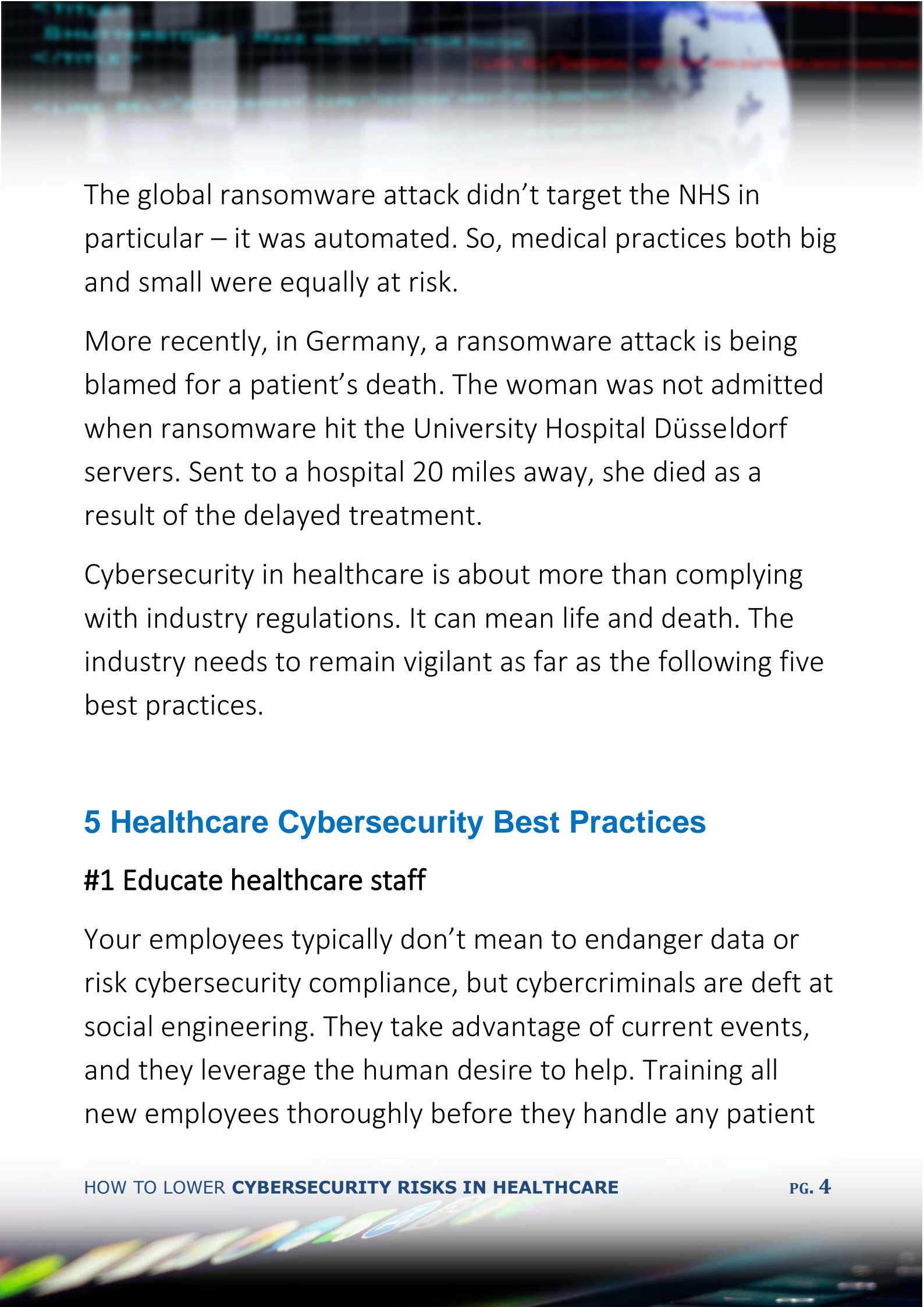
- 
- A BishopFox Labs researcher identified four vulnerabilities in OpenClinic health record management software.

These three examples help to show the range of issues healthcare providers face. Then, there's the risk of ransomware, which continues to plague the healthcare sector.

Consider the WannaCry Ransomware attack of May 2017 that preyed on a Windows XP vulnerability. Microsoft released patches shoring up its operating systems two months beforehand, but only to supported systems, and security fixes for Windows XP stopped in April 2014. Yet enormous numbers of machines were still running XP.

This included the National Health Service in the UK, which was hit hard. A 2019 impact report found the attack cost:

- £4million in lost inpatient admissions;
- £0.6million from lost accident and emergency activity;
- £1.3million from cancelled outpatient appointments.



The global ransomware attack didn't target the NHS in particular – it was automated. So, medical practices both big and small were equally at risk.


More recently, in Germany, a ransomware attack is being blamed for a patient's death. The woman was not admitted when ransomware hit the University Hospital Düsseldorf servers. Sent to a hospital 20 miles away, she died as a result of the delayed treatment.

Cybersecurity in healthcare is about more than complying with industry regulations. It can mean life and death. The industry needs to remain vigilant as far as the following five best practices.

5 Healthcare Cybersecurity Best Practices

#1 Educate healthcare staff

Your employees typically don't mean to endanger data or risk cybersecurity compliance, but cybercriminals are deft at social engineering. They take advantage of current events, and they leverage the human desire to help. Training all new employees thoroughly before they handle any patient



data is critical. Create and document a training program, and equip people to make smart decisions and use appropriate caution.

#2 Limit access

Limiting user access to a needs-only basis can help cut damage in the event of human error or a breach. Install access restrictions that require multi-factor authentication.

Ensure authorized users can access necessary patient information and certain applications only.

This includes access controls for:

- all network/server equipment and systems to prevent access and disclosure of patient data;
- software applications that contain patient data.

Create access and activity logs, and routinely review the logs for suspicious events and respond appropriately. Also, stop user accounts when necessary and appropriate.



#3 Encrypt data

Data encryption is essential at rest and in transit. This makes it difficult to decipher patient information if attackers gain access.

#4 Keep an accurate, thorough technology inventory

Analyze security risks and vulnerabilities. Inventory all systems, programs, and applications that store, send, or receive patient data. This requires securing mobile devices and all those IoMT devices, too.

Securing internet-connected devices requires tactics such as:

- managing all devices, settings, and configurations;
- enforcing the use of strong passwords;
- enabling the ability to remotely wipe and lock lost or stolen devices.



#4 Monitor partners, too

Healthcare information gets transmitted between providers and partners to facilitate payments and deliver care. Regular review of vendor and third-party service provider credentials should be ongoing.

#5 Conduct risk analysis

Assess risk and develop a risk management plan to address any identified vulnerabilities.

A managed service provider (MSP) can help with healthcare security and maintaining compliance.

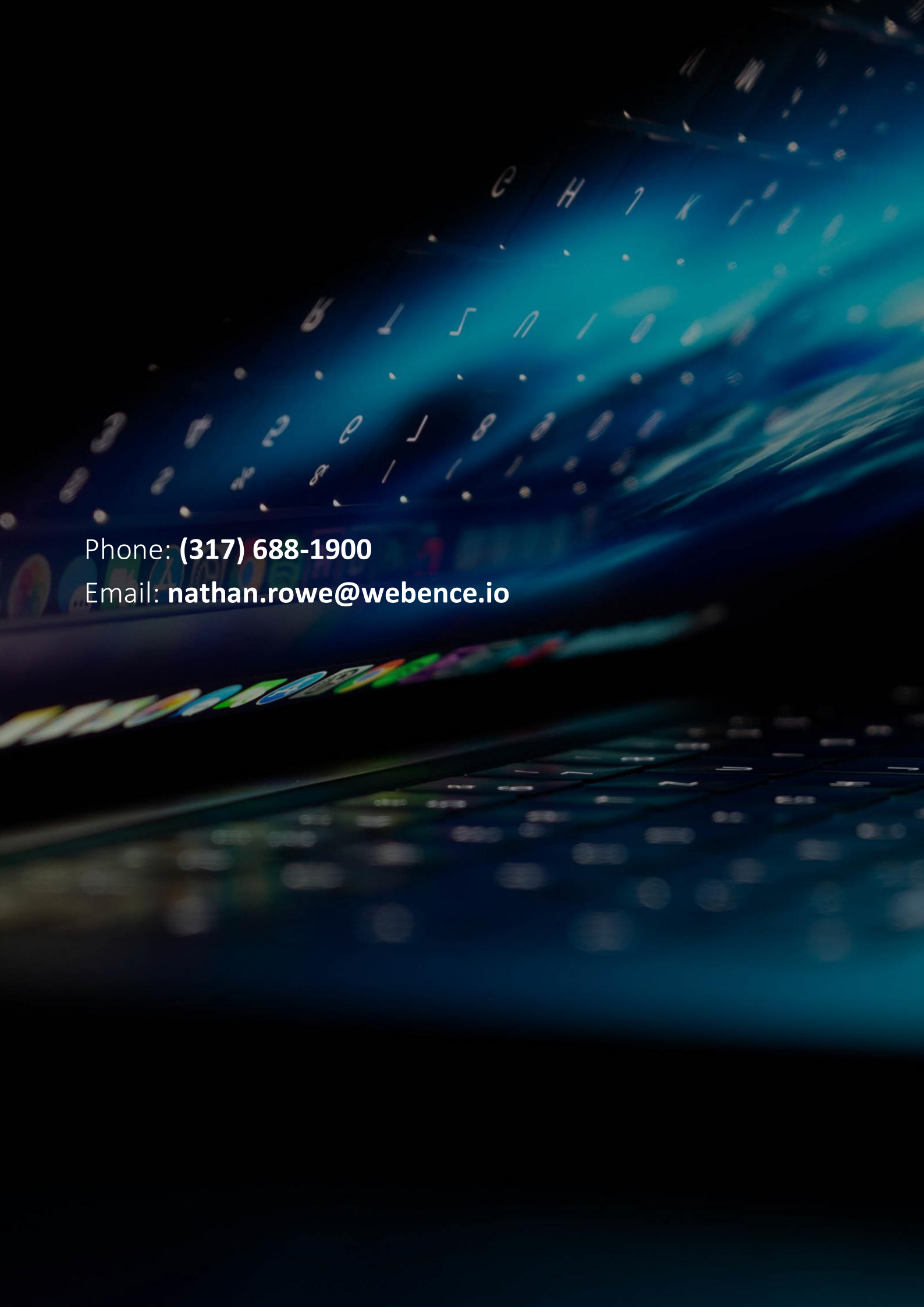


How a Managed Service Provider Helps

A partnership with an MSP can help healthcare providers shore up their cybersecurity. These IT experts can ensure the best practices enumerated above. Your MSP also takes proactive measures to help prevent future attacks.

The MSP allows doctors, dentists, therapists, orthopedists, and more to focus on keeping people healthy. Meanwhile, the MSP manages and monitors the IT for vulnerabilities. While keeping up with the latest threats to the industry, an MSP can also make a difference on a day-to-day basis. They recommend technology that helps healthcare providers work more efficiently, and they suggest secure solutions to streamline workflow, enable collaboration, and provide portable access.

Finally, an MSP can bolster data backup procedures and help establish continuity plans. That way, if the worst should happen, the healthcare provider can get you back up and running quickly.



Phone: **(317) 688-1900**

Email: **nathan.rowe@webence.io**