HEALTH CARE HELD HOSTAGE

Arming your business to defend against cyberattacks

WHITE PAPER

THE VGM GROUP
MEMBER SERVICE ORGANIZATION

ABSTRACT

The health care industry has become one of the top, if not THE top target for hackers. Health care data is rich with information hackers can exploit to make money.

Businesses in the health care industry are typically some of the larger employers in the community. Training a staff with a wide-range of technological experience is challenging, but it should be a priority.

According to McAfee, **43 percent of all company data loss or breaches are caused by employees.** How many of your employees have access to email? Opening something as routine as an email attachment can expose your network to hackers.

The costs of a breach are skyrocketing across all industries, and breach-related fines from the government are greater than expected. **Fines for data breaches have ranged from $500 to $2,500 (estimated) per record**, depending on the government agencies involved, fees, and patient notification expenses. One health care provider lost 412 patient records and paid $650,000 in fines alone. In fact, insurance experts estimate that 60 percent of small businesses will go out of business within a year of having a major data breach.

Remember, hackers work full time, searching for ways to penetrate a business's infrastructure to capture company and patient data. They will do anything they can to gain financially from IT oversight. Don't risk it all. Arm yourself with these tools and practices to protect your business from online threats.

1. **Invest time and resources into developing and regularly updating IT policies. Technology changes in a blink of an eye, and your policies should reflect those changes.**

2. **Hire third-party security experts to expose known threats through penetration testing.**

3. **Train your staff to be your strongest line of defense against hackers.**

4. **Purchase Cyber Liability Insurance to cover your liability for a data breach.**

INTRODUCTION

In a time when cyberattacks threaten every business and organization, it has never been more important for the health care industry to prioritize cybersecurity.

The health care industry has become one of the top, if not THE top target for hackers. Health care data is rich with information hackers can exploit to make money. Health care records typically contain very sensitive information including patient name, current address, SSN, DOB, insurance/Medicare ID, cell phone number and credit card or checking account number. Each of those personal data points is valuable on the cyber black market and, aggregated, are even more valuable.

In this white paper, Jeremy Kauten, CIO and Senior Vice President of IT for VGM Group, Inc., writes about the current state of affairs in cybersecurity, how to determine levels of risk to your company and patient data, and provides best practices to help protect your business from hackers.

Current environment of cyber threats

While data breaches at large businesses such as Target, Anthem, Yahoo and major health systems often make the headlines, the majority of data breaches affect small businesses throughout the U.S.

Typically, small businesses do not have the resources to organize and fund a sophisticated IT security program. Hackers know this, which gives them an advantage when targeting a business to attack. Most unsuspecting victims find out about an attack when it's too late. In fact, **insurance experts estimate that 60 percent of small businesses will go out of business within a year of having a major data breach**.

Over the years, hackers have become more business savvy. They operate as a stand-alone hacking entity or under a legitimate business as a front. They even offer their employees full benefit packages.

One of the latest forms of cyberattacks is known as ransomware. This attack involves hackers encrypting data, meaning it is locked, and then requesting a ransom payment to unlock the files/data. According to the FBI, ransomware payments alone exceeded $1 billion in 2016. Ransomware hackers often offer 24/7 tech support to help their victims get up and running again. They don't want to "tarnish their industry" by not delivering once the ransom has been paid.

The costs of a breach are skyrocketing across all industries, and breach-related fines from the government are greater than expected. **Fines for data breaches have ranged from $500 to $2,500 (estimated) per record**, depending on the government agencies involved, fees, and patient notification expenses. One health care provider lost 412 patient records and paid $650,000 in fines alone.

In the event of a security breach, health care providers can expect an added expense to comply with HIPAA Privacy Rules (45 CFR 160-164) and HITECH (Health Information Technology for Economic and Clinical Health) standards. *Note: The HITECH Act requires data breach notification for disclosures of unsecured PHI (protected health information) within 60 days of enactment.*

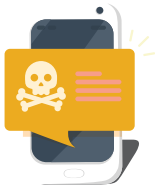
In addition to fines, there are tangible and intangible expenses attached to alerting patients and the media of the breach.

One major expense that is not often considered is *brand reputation*. Imagine trying to get referrals from an insurance company or health system when it is public information that a provider's system had been compromised. The negative effect on brand reputation alone and associated lost revenue is likely the most damaging to a business.

Identifying your greatest risk

Most, if not all health care providers would agree that their greatest assets are employees. When it comes to patient care, they're probably correct.

When it comes to cybersecurity, however, employees are the biggest threat to data security. According to McAfee, 43 percent of all company data loss or breaches are caused by employees. By simply clicking on an attachment or link in a malicious email, using unsecured Wi-Fi with their mobile device(s), or misplacing documents, employees can inadvertently open a business up to a significant financial loss.



Alarming statistics confirm why hackers target small businesses. **According to the Small- to Medium-size Business Threat Awareness Poll, 67 percent of small- to medium-size businesses do not use web-based security, and 61 percent do not use antivirus on all computers.** Phones, tablets, computers and laptops typically access the infrastructure and at some point contain patient data or access to patient data.

- Software updates and proper protection on devices do not require an IT expert and are crucial to protecting company and patient data.
- Security experts agree that a business's computer systems and networks, or infrastructure, must be addressed in a cybersecurity program. Protect your infrastructure by using proper firewalls, anti-virus, web filtering, email filtering, access levels, as well as by making smart decisions about the software you're using to store patient data.
- Software systems, such as billing or patient management software, are another element of risk. Most providers use third party, cloud or hosted software and rely on their software vendor for security.
- When using a third party-hosted software, two-factor authentication should always be turned on when available. This is one line of defense, but don't stop there. Networks need to be able to protect files locally as well software that is hosted elsewhere.

Best practices to protect your business

In today's environment of data-driven business solutions, it has never been more important for small-business owners to be proactive in understanding threats to their business and invest in data breach protection.

Cybersecurity threats are an ever-evolving problem. Health care providers should be creating and updating IT policies to address newer technologies and the increasing cybersecurity threats. Policies should be reviewed at least annually, and any revisions should be communicated to staff members.

Technology is an intimidating and complicated business tool. Coupled with other day-to-day business practices, it's difficult for the average health care provider to keep up on the latest threats.

Hiring third-party security experts to expose known threats and offer best practices is necessary for health care companies. There are companies that specialize in ongoing penetration tests where a white hat hacker (an ethical computer hacker or security expert) will attempt to breach a system. Following the test, the vendor will provide a detailed report of vulnerabilities. This report can serve as a resource for developing and implementing security measures to protect data.

Training staff is vital to protecting data. Employees who are trained on how to handle potential cyber risks can protect a company by carrying out a secure culture. If we compare this to TSA, which educates travelers to keep an eye out for suspicious behavior, employees should be expected to do the same to protect a business from suspicious activity.

A number of easy-to-use and trackable training programs are available to help educate staff. Regular training helps to build an additional line of defense to ensure company and customer data remain secure and protected from hackers and other online threats.

A business's billing software likely houses all pieces of valuable patient data. Most software allows for IP lockdown so that it can only be accessed via the company's protected network or offsite through a secure VPN (virtual private network) connection. And again, when using a third-party hosted software, two-factor authentication should always be activated.

Finally, health care providers should consider purchasing a Cyber Liability insurance policy. Cyber policies can cover a business's financial liability for a data breach. During the process of acquiring a cyber policy, the insurance company will typically go through a list of best practices with you and can even offer additional training resources.

CONCLUSION

Cybersecurity is something that should be taken very seriously. Hackers work full time to find ways to penetrate a business's infrastructure to capture company and patient data. They will do anything they can to gain financially from IT oversight. Don't risk it all. Arm yourself with tools and practices to protect your business from online threats.

For more information and additional resources, visit www.vgm.com/security.

About the Author

Jeremy Kauten serves as Chief Information Officer and Senior Vice President of Information Technology for VGM Group, Inc. His responsibilities include leading VGM's corporate Information Technologies department, coordinating optimization of technology, strategizing on how to accelerate success across VGM's 28 business units and spearheading the technology message to share with the membership groups.

Jeremy's energy, leadership and ability to bring people together augment the development of systems and technology across VGM. He has developed and implemented thorough internal and external training programs to educate management, staff and customers alike to ensure company and customer data remain secure and protected from hackers and other online threats. Jeremy has presented at various health care tradeshows and state association meetings throughout the U.S.

Contact Information
Jeremy Kauten
CIO and Sr. VP of IT, VGM Group, Inc.
1111 West San Marnan Drive
Waterloo, Iowa 50701

319-274-4438
Jeremy.Kauten@vgm.com
www.vgmgroup.com