THE AGENCY REVIEW 2016 • Issue I

CYBERATTACKS
THE Y2K OF THIS DECADE:
This time, the threat is REAL.

By Tammi M. Arrington, Account Manager

According to a report by Raytheon/Websense, the healthcare industry has 340 percent more security incidents and attacks than most other industries. It's no secret that medical offices maintain scores of records containing protected health information (PHI). PHI is much more attractive than other forms of data to cyber criminals because the value per record is greater. Retail stores may hold credit card numbers without any other identifiable information, but medical records contain social security numbers, credit card numbers, addresses, full names, dates of birth, etc., making it easier for criminals to recreate profiles. Further, the healthcare industry has admitted it has fewer resources to devote to the security of its computer systems (due in part to lower reimbursement and regulatory demands), thus making healthcare a prime target for future attacks.

There are various types of cyberattacks, the most common of which within the healthcare industry is called ransomware. Ransomware is malicious software that prevents or limits users from accessing any electronic records.

CryptoLocker and CryptoWall are the forms of ransomware mostly seen in the U.S. today. On Sept. 16, 2015, a Medical Assurance Company of Mississippi (MACM) insured clinic discovered that a ransomware virus had attacked its computer system and locked its electronic medical records. The clinic staff was unable to access medical records and files.

The clinic's IT vendor was able to determine that the violation occurred at one computer where personnel discovered a ransom note for $400 payable by bitcoin to unlock the clinic's patient records and files. Bitcoin is a quasi-black market form of electronic currency which is difficult, if not impossible, to trace. It is an uncommon form of payment to be sure, but it can be done with the help of IT experts. After multiple attempts were made over a two-day period to reconstruct the files, the clinic chose to pay the ransom. The clinic then learned that due to the delay, the ransom had been increased to $1,000, so a decision was made to satisfy the demand. Once the ransom was paid, the account was unlocked, and the patients' records were, once again, accessible. The IT experts confirmed that the information contained in the files had not been accessed, resolving any concerns about a potential HIPAA violation. Fortunately, the clinic had a cyber coverage policy with MACM, through NAS Insurance Services, LLC, which covered the ransom, the independent IT vendor expenses, wages of employees who assisted with reconstructing the data, and the cost to restore the firewall.

How does a cyberattack occur?

One of many ways the malware can infect your computer happens when you click on a legitimate-looking attachment or through existing malware lurking on your hard drive. Once opened, it instantly locks all your files, restricting access to a single file on your computer. Unsolicited emails containing an infected file posing as a voicemail or shipping confirmation are widely used to distribute Cryptolocker/CryptoWall. The virus can also infiltrate your computer via malicious web ads (malvertising).

THE HEALTHCARE INDUSTRY HAS

340%

MORE SECURITY INCIDENTS AND ATTACKS THAN OTHER INDUSTRIES.

What to expect once a cyberattack has occurred?

Typically, what occurs after files are encrypted is that an official-looking warning, including a ransom note, is delivered. Such a ransom note might read, "Your files have been encrypted. To get the key to decrypt files you have to pay $500 USD." The virus may contain a countdown clock indicating a proposed time frame in which to pay the ransom. Failure to pay within the time allowed typically results in the ransom being increased. Failure to pay the ransom altogether can lead to the decryption key being destroyed and access to the data being lost forever.

Is there any way to unlock your files instead of paying the ransom?

At present, the answer is no. It appears to be technologically impossible for ANYONE to decrypt your files once they have been locked. MACM has been in contact with the FBI following an attack on one of our clinics, and the response was not encouraging. They implied that the relative-

"Bitcoin is different than any currency you've used before, so it's very important to understand some key points. Unlike government issued money, that can be inflated at will, the supply of bitcoin is mathematically limited to twenty one million bitcoins, and that can never be changed. Bitcoins are impossible to be counterfeited or inflated. You can use them to send or receive any amount of money, with anyone, anywhere in the world, at very low cost. Bitcoin payments are impossible to be blocked, and bitcoin wallets can't be frozen. Short of turning off the entire world's internet, and keeping it turned off, the Bitcoin network is unstoppable and uncensorable. While Bitcoin brings unparalleled freedom, it also requires increased user responsibility."

source: bitcoin.com

ly low monetary demands made in connection with these attacks make them low priority cases. The FBI wants companies to know that the Bureau is there for them if they are attacked; however, if that attack involves Cryptolocker, Cryptowall, or other forms of ransomware, the nation's top law enforcement agency is warning companies they may not be able to get their data back without paying a ransom.

How can MACM help?

In January 2016, former FBI director, Robert S. Mueller III, warned that "nobody is going to avoid being hacked. It's just a question of how severe the breach will be." Even after taking all of the above steps in order to avoid cyberattacks, you are still in danger. This is where your coverages with MACM and MACM Insurance Services are here for you and your practice.

Since January 1, 2012, MACM has provided its clients with cyber liability protection in addition to their professional liability coverage. This protection provides $100,000 of coverage for each physician. If a clinic is interested in additional limits, then MACM's subsidiary agency, MACM Insurance Services, can handle the request. For a nominal fee, approximately $400 for a solo practice, a physician can buy an additional $1 million limit of cyber liability protection. A group premium is dependent on the number of providers within the organization, but the larger the group, the lower the per-provider cost.

Physician insureds also have access to a website dedicated to providing information geared towards minimizing the risks of cyber liability. Should a claim arise, you can be sure that it will be handled quickly and in the same professional manner that you have already come to expect from MACM.

Cyber liability is at the forefront for claims and lawsuits these days. Protect yourself and your clinic with a phone call to the staff of MACM Insurance Services at (601) 605-4882 to put your mind at ease today.

HOW CAN YOU **REDUCE** THE RISK OF A CYBERATTACK?

The best defense against cyberattacks and the most effective way to protect your patients' information is to engage in nightly data backups.
This protects the information and provides a framework to rebuild if a breach occurs. The following are suggestions to aid in protecting your valuable data:

- Have procedures in place for regularly backing up your data. It is preferable to have nightly backups. This removes the need to pay any ransom if a breach occurs.
- Keep computers backed up on an independent drive or by using a cloud backup service like Carbonite.
- Use and maintain antivirus and anti-malware software. Take software update alerts seriously. Don't neglect your IT security software updates — even when it costs additional fees to upload.
- Keep your operating system and application software up-to-date. Install software updates so attackers can't take advantage of known problems or vulnerabilities.
- Beware of email attachments. It is the attachment to the email that contains the potential hazard. If the attachment came from an unknown sender either unexpectedly or unsolicited, the best decision would be to delete the email without opening it. If the email is from a known and trusted source, but you did not expect an attached file from that source, you may want to contact the sender to confirm that the attachment is legitimate. Also, beware of any retail stores sending coupons as attachments. Major retail stores will only send coupons that are embedded into the email, not as an attachment.
- Be wary of any emails stating that you are receiving a package when you are not expecting any shipments.
- Decrease user error by developing policies and procedures for cybersecurity and hold security awareness training sessions. This is critical to demonstrating the importance of cybersecurity to staff.
- Implement protocols. For example, hover over hyperlinks to ensure that all domains are the same, or pay close attention to the domain of the email sender. The domain name could only be off by one or two letters or end with .com instead of .net. For instance, if you regularly receive an email from John.Doe@macm.net, there would be cause for concern if you received an email from John.Doe@maaccm.net or John.Doe@macm.com.
- A layered approach to antivirus and anti-malware software is suggested for your computer systems. The MACM IT department recommends the following:

1. **Anti-Malware**: software that identifies and removes malware and eliminates malware.
   - **Malwarebytes** – www.malwarebytes.org/ — also good to use to clean up a computer that might have malware on it.
   - **SUPERAntiSpyware** – www.superantispyware.com

2. **Antivirus**: software that recognizes and protects your computer against most known viruses.
   - **ESET** – www.eset.com/us/ — Antivirus, Internet Security Software & Virus Protection
   - **AVG** – www.avg.com/ — Free antivirus protection
   - **Trend Micro** — www.trendmicro.com – Antivirus + Security Software

- Secure Your Network Connection: Offer a password-protected courtesy network for guests or employees who would like to check personal email, social media, and browse the internet in their free time or while waiting to be seen by a provider. An IT consultant can help set up secure and courtesy wireless networks within your practice.

  Regularly change the network password to assure accessibility is limited to those for whom it is intended. Consider establishing a monthly reminder for office managers to update the network password settings and redistribute credentials to authorized staff on a regular basis.

Krista Ely

SUN COAST PAIN MANAGEMENT

SEEKS PROTECTION WITH BILLING E&O AND EPL COVERAGE

> "The staff has always kept us up-to-date on any product that might be beneficial and that is how we ended up working with the staff of MACM Insurance Services."

For Krista Ely, clinic administrator for Sun Coast Pain Management in Ocean Springs, the relationship with a company is just as important as the price. And, the long-term relationship with MACM is what led her to MACM Insurance Services.

Since 2009, Ely has purchased supplemental products from MACM Insurance Services to complement the medical malpractice coverage her physicians purchased from MACM. These additional insurance products provide her and the physician management with the level of comfort they need to know they are protected on the business side of the clinic.

"We have had a very close relationship with MACM for a long time, and when I had questions about things going on in the clinic, I could call," Ely said. "The staff has always kept us up-to-date on any product that might be beneficial and that is how we ended up working with the staff of MACM Insurance Services."

For Ely and clinic owner, Y.C. "Joe" Chen, MD, the need to protect Sun Coast Pain Management from inadvertent errors in the billing process, as well as personnel issues, was important. To alleviate this worry, Ely worked with the MACM Insurance Services staff to bundle several coverages together – Billing Errors and Omissions (E&O) and Employment Practices Liability – to provide the clinic with the protection needed.

The Billing E&O is insurance that protects a clinic against RAC audits of Medicare/Medicaid billing and HIPAA violations.

Krista Ely and Joe Chen, MD

Intentional (and unintentional) over-billing of Medicare and Medicaid is a prime target for federal regulators. In addition, rules governing the restricted use of patient information can create additional liability exposure for healthcare providers like Sun Coast Pain Management. Billing E&O coverage provides protection for these types of allegations as well as coverage for defense costs, auditing fees, and civil fines and penalties.

Sun Coast Pain Management also realized a need to be conscious of the risks associated with handling personnel issues and thus purchased Employment Practices Liability (EPL) – insurance that covers alleged wrongful acts arising from the employment process. With EPL, coverage is provided for the clinic when claims are brought by past, present, and potential employees. This policy is designed to protect against these common allegations: discrimination in the hiring process, sexual harassment, failure to promote, and wrongful termination.

The application process is simple and allows MACM Insurance Services to shop for the best price and most complete coverage. If you are interested in Billing E&O or EPL coverage, contact MACM Insurance Services at (601) 605-4882.

macm
INSURANCE SERVICES
404 West Parkway Place
Ridgeland, Mississippi 39157
www.macm.net
601-605-4882
mis@macm.net

PRST STD
U.S. POSTAGE
PAID
Jackson, MS
Permit No. 775

A subsidiary of Medical Assurance Company of Mississippi

TAMMI M. ARRINGTON AND CHARITY HUSTON ADDED TO MACM INSURANCE SERVICES STAFF

MACM Insurance Services is pleased to announce the addition of two staff members now available to assist our agency insureds.

Tammi M. Arrington is an Account Manager with MACM Insurance Services and is responsible for managing the outside sales efforts. She joined MACM in 2013 where she currently serves as the Marketing Representative. Tammi holds her Mississippi Property & Casualty insurance license. Prior to joining MACM, Tammi attended Mississippi State University and worked over 13 years in clinic administration, primarily with surgical specialties.

Charity Huston is an Account Manager with MACM Insurance Services and available to assist the agency's current insureds with policy changes and the renewal process. Charity holds her Mississippi Property & Casualty insurance license. She received her Associate in Applied Science Degree in 2009 and is a Registered Radiologic Technologist. She worked in the medical field from 2008 until she joined MACM in 2015.