PROTECTING YOUR ORGANIZATION FROM CYBER ATTACKS

Gallagher

Insurance | Risk Management | Consulting

Senior Living

Jane C. Feagin, BSN, RN, ALA, RMC, CDP
Loss Control Specialist

CYBER ATTACKS ON THE RISE

Cyber, cloud computing, cookies, anti-virus, ransomware, malware, breach and hacked… the list goes on and on. Cybersecurity is something that many of us have not heard until recently, let alone dealt with. Yet here we are in a cyber-driven world.

In particular, ransomware has become an extremely hot topic. This is a malicious software that encrypts a victim's data, making it inaccessible until a ransom is paid. It is becoming a more common occurrence for the healthcare and senior living industry. The Ponemon Institute cites that "Criminal attacks are the leading cause of data breaches in healthcare, and healthcare organizations report 50% of their breaches come from cyber attacks."[1]

A cyber attack can start with an action as simple as clicking on an email attachment or link that is "malicious." Once you have clicked on that malicious email, you have now opened your network up to a quickly spreading software that locks down files throughout the organization. Hackers, or the person with knowledge to analyze your program and modify the functions of your operating system, leading these criminal attacks, are now in control and are demanding ransom payment before they will release your data. Sadly, there is no guarantee that if you pay, your data will be released. And sometimes even if your data is released, it may be encrypted and is no longer useful.

"The average ransomware payment for the Healthcare and Public Health sector is $131,000. The average bill for rectifying a ransomware attack — considering downtime, people time, device cost, network cost, lost opportunity, ransom paid, etc. — was $1.27 million."[9] Ransom amounts have nearly tripled in just a years' time with the average ransom within one year going from the beginning of the year at $5,900; to at the end of the year to $36,300.[2] That is quite a jump in the dollar amount! And since more than half of breaches are financially motivated, you must add in the many other costly and time consuming details, such as decryption of your data.

Ransomware attacks in which hackers hijack your computer system or website and demand payment to release your information is on the rise. Cyber attacks, i.e. 'ransomware, has impacted at least 621 entities this year,[2] with targets being hospitals, healthcare centers, school districts and cities.

These attacks have closed schools, delayed surgeries, delayed home sales, issues in bill payments and stopped staff from doing their jobs. "There is no reason to believe that attacks will become less frequent in the near future."[2] So why have ransomware attacks been on the rise in recent years? Primarily due to the high profitability for the hackers.

Medical records are valuable, ranging from $500 to $1000 per record. Records can also contain a large amount of personal information that can be used for items such as blackmail, identity theft, or fraudulent insurance claims. Also, it may take an organization around a 197 days to detect a breach, with a mean time to contain the breach of roughly 69 days.[10]

GAINING ACCESS

Let's Talk Privacy

Health Insurance Portability and Accountability Act (HIPAA) is a federal law that restricts access to an individuals' private medical information; the U.S. Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. "The privacy rule standards address the use and disclosure of individuals' health information, also known as "protected health information" by entities subject to the Privacy Rule. The Privacy Rule also contains standards for individuals' rights to understand and control how their health information is used."[3]

The following types of individuals and organizations are subject to the Privacy Rule and considered covered HIPAA entities:

- **Healthcare providers:** Every healthcare provider, regardless of size of practice, who electronically transmits health information in connection with certain transactions. These transactions include claims, benefit eligibility inquiries, referral authorization requests, and other transactions for which HHS has established standards under the HIPAA Transactions Rule. (Examples include: physician practices, hospitals, and skilled nursing facilities.)

- **Health plans:** Entities that provide or pay the cost of medical care. Health plans include health, dental, vision, and prescription drug insurers; Health Maintenance Organizations (HMOs); Medicare, Medicaid, Medicare+Choice, and Medicare supplement insurers; and long-term care insurers (excluding nursing home fixed-indemnity policies). Health plans also include employer-sponsored group health plans, government- and church-sponsored health plans, and multi-employer health plans.
- **Healthcare clearinghouses:** Entities that process nonstandard information they receive from another entity into a standard (i.e., standard format or data content), or vice versa. In most instances, healthcare clearinghouses will receive individually identifiable health information only when they are providing these processing services to a health plan or healthcare provider as a business associate.
- **Business associates:** A person or organization (other than a member of a covered entity's workforce) using or disclosing individually identifiable health information to perform or provide functions, activities, or services for a covered entity. These functions, activities, or services include claims processing, data analysis, utilization review, and billing.[3]

Any information relating to past, present or future physical or mental health condition of an individual, provision of healthcare to an individual or past, present or future payment for healthcare for an individual is considered "PHI" or Protected Health Information. This information can be written, verbal or electronic i.e., medical records, medical billing records, and patient demographic information.

As we mentioned above, hacking or IT incidents account for more than 45% of the breach reports with an impact from breaches being an estimated average of $3.86 million.[1] This included PHI exposed on the internet, with 24% of data breaches today occurring in the healthcare sector.[6] We have all heard about companies that have suffered huge losses that affected millions of people due to breaches from cyber attacks and you do not want to find your company in this position.

Internet of Things

Basically, Internet of Things (IoT) is a system of devices and things that are implanted with sensors, software and electronics to initiate the exchange and collection of data and information. The reason why we connect these objects is simple: for convenience. Approximately 30.3% of IoT devices are used in the healthcare industry,[7] from portable health monitoring to serving as a safety measure for personal records.

PROTECTING YOUR ORGANIZATION

Cyber risk are lurking around and you do not want to put your residents or your organization on shaky ground because of unwanted attention from hackers. Below are some questions you should ask yourself:

Do we have backup of our data?

Is the backup stored off-site?

Do I have a cyber attack team?

Where is the teams contact information stored?

Does your facility have a cyber risk assessment that is completed either by your IT department, your cyber risk team or an outside vendor?

Preventing cyber attacks is not an easy task. Typically, providers are not the most-sophisticated in cybersecurity which requires planning, auditing and analysis of information as well as training.

Training

Most breaches may have been avoided if there had been proper training. Therefore, it is important to implement a thorough cyber training program. Below are some tips to consider when developing your program.

- Implement security measures, like what to do and what not to do, such as leaving your computer unattended or sharing access to your computer.
- Include the little things. Some actions that may sound simple and like something you or your staff would never do, but it happens.
- Training of all staff should begin as each new employee is hired.
- Educate staff on what a suspicious email may look like. This could include numerous spelling, punctuation or grammar errors.
- Make sure your staff knows what they should do and who they should notify should they receive a suspicious email.
- Promote the importance of using strong passwords. This is a simple and easy way to manage and lower your risk of cyber attacks.
  - » Change your password frequently.
  - » Use uncommon passwords.
  - » Create a password of integrity.
  - » Never share your password with anyone.
  - » Never write your passwords down and save at your workstation.

Educating your staff on the possible pitfalls of something as simple as opening an email that is suspicious, may be all it takes to avoid an attack.

49% of non-point of sale malware is installed via a malicious email.[6]

Other Considerations

- Control physical access to your information. If computers are secure and inaccessible, then this will lower the ease of violating your information. Never leave laptops in your car, this is just too easy for someone to pick up and go.
- Be proactive, before your data is compromised by having a cyber risk assessment.
- Have a plan and have a cyber-team in place.
- Look at ways you can monitor your potential cyber risks. Are you performing a Cyber Risk Analysis?
- Review your current insurance policy for cyber coverage gaps. If you don't currently have a cyber policy, consider purchasing one.
- Know your company policy on breaches in case one does occur like do you pay the ransomware or not?

As long as there are cyber hackers that continue to exploit the increased use of computer systems, a lifeline for many companies and organizations, there will be cyber attacks and ransoms. That is why it is important to prepare your company for the many vulnerabilities that exist in this ever changing environment.

Sources:

[1]Ponemon Institute. Annual Benchmark Study on Privacy & Security of Healthcare data. May 2018.

[2]Ransomware's mounting toll: Delayed surgeries and school closures; Fabian Wosar, CTO at Emsisoft; October 2, 2019/Moneywatch

[3]https://www.cdc.gov/phlp/publications/topic/hipaa.htm Health Insurance Portability and Accountability Act of 1996 (HIPAA)

[4]Primer on HIPAA Requirements for Business Associates Protecting PHI: The Buck Stops Here for BAs. Clearwater Healthcare Cyber Risk Management

[5]https://www.hhs.gov/hipaa/for-professionals/faq/2075/may-a-hipaa-covered-entity-or-business-associate-use-cloud-service-to-store-or-process-ephi/index.html

[6]https://safeatlast.co/blog/data-breach-statistics, 30 Horrific Data Breach Statistics and the Biggest Breaches.

[7]https://safeatlast.co/blog/iot-statistics 80 Insightful Internet of Things Statistics (Infographic)

[8]Alabama Nursing Home Association Defense Lawyers Meeting, April 2019 Presentation. Jim Hover and Kelli Fleming of Burr & Foreman LLC

[9]https://www.hhs.gov/sites/default/files/ransomware-trends-2021 HHS Cybersecurity Program Ransomware Trends 2021

[10]https://www.varonis.com/blog/data-breach-response-times/#:~:text=On%20average%2C%20companies%20take%20about,to%20those%20who%20take%20longer.

Jane C. Feagin

About the Author.

Jane C. Feagin is a Loss Control Specialist for the Senior Living Risk Partners Division of Gallagher Risk Management Services. She received her Degree in Nursing from Jefferson State Community College in Birmingham and her BSN from Auburn University, Montgomery. Jane has worked in healthcare for more than 30 years where the Senior Living industry has been Jane's primary focus for the past 20 years. She has held various positions including Director of Healthcare — Assisted Living, Director of Marketing — Home Health and Hospice, Referral Development Coordinator for Long Term Acute Care Hospitals, Long Term Care Unit Manager, Resident Assessment Nurse — SCALF, Specialty Pharmacy/ Infusion Liaison, as well as direct patient care provider. Jane also holds a Category II Assisted Living Administrator's License for Alabama and an Assisted Living Administrator License for Florida. She is a Risk Manager Certified and in 2017, she received her certification as a Certified Dementia Practitioner from the National Council of Certified Dementia Practitioners and has completed the Nursing Home Infection Control Prevention (NIPP) training program with RB Health Partners.

Jane C. Feagin, BSN, RN, ALA, RMC, CDP
Loss Control Specialist
Senior Living Practice
2200 Woodcrest Place, Suite 250
Birmingham, AL 35209

205.414.2595
jane_feagin@ajg.com

Connect With Us

Jane Feagin

Loss Control Specialist
BSD - Birmingham

2200 Woodcrest Place
Birmingham, AL 35209
T: 205-414-2595
E: jane_feagin@ajg.com

ajg.com **The Gallagher Way.** Since 1927.

Gallagher