HOW TO PREPARE FOR A CYBER BREACH

By John Southrey, CIC, CRM, Director, Product Development and Consulting Services, and
Wayne Wenske, Senior Marketing Coordinator

Data breaches continue to be rampant in health care, and the financial impact to physicians and patients can be greater than expected. It is widely known among cyber criminals that health care organizations generally have limited security budgets and inadequate data safeguards making them easy targets for cyber attacks.[1]

As the use of various forms of technology — such as Internet-connected medical devices and health data sharing — increase throughout health care, so will cyber risks. And the direct and indirect costs of a breach incident can be devastating.

Direct costs of a breach can include:

- fees for legal counsel;
- IT forensic expert fees;
- breach notification expenses;
- third-party damages; and
- regulatory fines and penalties.

Indirect costs can include:

- loss of income;
- expenses to deal with the incident; and
- potential loss of revenue from reputational harm caused by adverse media about the breach.

CLOUD-BASED BREACHES

Breach incidents can occur on- or off-premises, including "in the cloud." Therefore, moving data to the cloud does not eliminate cyber risks.

More health care organizations are relying upon uninterrupted access to cloud-based information to conduct their operations. If a cyber attack causes the cloud's network to go down, this dependence can expose medical practices to a damaging business interruption.

This kind of breach can be especially disruptive for a practice without contemporaneous data backup, or if access cannot be restored in a timely manner. Even if the practice has a real-time backup, restoring corrupted data can take days or even weeks.

The recent Allscripts ransomware attack in January 2018 is a prime example. The attack shut down two data centers that hosted Allscripts' EHR systems and software used for the electronic prescribing of controlled substances. The shutdown lasted more than a week and interrupted services to approximately 1,500 health care organizations. Hundreds of physicians and thousands of patients were affected.

Many of the affected practices were small physician groups that began using paper records and manual processes to avoid interrupting patient care. One Allscripts customer shared, "we immediately convert[ed] to paper and [kept] moving forward. This time I created an appointment schedule on Excel and we manually put in several days of the schedule from the Mobile App and everyone has access to the Excel spreadsheet to see who is coming in and add appointments." [2]

While this type of solution is not ideal, it is important for practices to consider creating an incident response plan if an interruption to business operations occurs.

TIME DOWN EQUALS HIGH LOSS

According to research from Accenture and the American Medical Association, "Nearly two-thirds (64 percent) of all physicians who experienced a cyber attack experienced up to four hours of downtime before they resume operations, and approximately one-third (29 percent) of physicians in medium-sized practices that experienced a cyber attack said they experienced nearly a full day of downtime." [3]

How much a data breach can cost varies based on the size of the data loss and how quickly it is contained. A recent report from Ponemon Institute suggests that "response time means everything," and that the time it takes to identify and mediate a data breach can determine the final costs to an organization.[4]

A hypothetical example of a breach scenario that involved a cloud solution provider (CSP) suggests the following:

- Malicious code makes its way into a CSP, infecting 25-50 percent of the system.
- It takes 24 hours for security experts to mobilize and identify the entry point of the malicious code.
- It takes 24 hours to develop patches for the found vulnerability and system crashes.
- It takes another 24 hours for the next tier of security providers to help investigate, secure, and fix the problem.
- It takes 6 to 48 hours ramp-up time for security.
- One to 12 hours of additional time for affected companies to bring their systems online after the CSP has restored service.
- Total outage time: 55 hours *minimum*.[5]

According to a report from NetDiligence, "healthcare and professional services were the most breached sectors, each representing 18 percent of all breaches." In addition, the "average cost of a breach was $394,000— but in health care, the cost was much higher at $717,000." [6]

After a breach incident, the medical practice may experience a reduction in revenue due to a drop-off in patient appointments. A practice's failure to properly safeguard protected health information can lead to diminished patient trust.

WHO IS LIABLE FOR LOST OR COMPROMISED DATA?

Many Service Level Agreements used by CSP and EHR vendors include provisions that stipulate a *shared responsibility* with the customer for the security of the data being stored. Most CSPs will try to limit their liability for both service outages and breach incidents.

"Notably, the shared responsibility model leaves the cloud customer fully accountable for the data that is being stored outside the business, which in the event of a breach makes them most liable for any third-party damages or responsible for regulatory action." [7]

Therefore, it is advisable that health care entities carefully review third-party service contracts with legal counsel to determine exactly what damages they may be liable for in the event of a breach. Make sure you understand any contractual obligations with regard to liability assumed under contract, particularly as it relates to the use, disclosure, or safeguarding of your electronic protected health information (ePHI).

In a breach investigation, the U.S. Department of Health and Human Services' Office for Civil Rights would likely look first at the owner of the data's cyber security management and obligations. Depending on the circumstances, some or all of the following issues would be addressed.

- Who owns the data?
- Who notifies the affected individuals, local media, and regulatory authorities?
- Who pays for the notifications and press releases?
- Who pays for the forensics to determine the causation of the breach and if any personal data was stolen?
- Who pays for the credit monitoring and identity theft restoration services for the affected individuals?
- Do the contracting parties have cyber insurance that covers any liability assumed under contract?

Again, reviewing these contracts (including the above questions) with legal counsel, and amending them where possible, can help you minimize this liability and associated costs. It is also advisable to review your cyber liability insurance coverage to make sure it can fully protect you in the event of a business interruption.

RISK MANAGEMENT CONSIDERATIONS

The costs associated with a breach — whether it is onsite or in the cloud — can be devastating. Therefore, it is important to understand affiliated costs of a breach; minimize your liability by reviewing and amending third party service agreements; assess your current cyber liability coverage to determine if it meets your current needs; and stress the importance of cyber risk management for your practice.

The following risk management considerations can help you avoid or manage a cyber breach.

- **Educate staff members.** Unfortunately, many cyber breaches occur because of human error. An employee may click on a link in a phishing email because he or she does not know any better. While many employees may be fully aware of online risks, others may not be educated on the matter. This knowledge gap can leave a practice open to cyber risks from malicious email campaigns and poorly managed passwords.

  Train staff members on the measures they can take to prevent data breaches. One such campaign could be on how to identify a phishing email and instructing staff to never click on a link sent by an unknown sender or open an attachment that was not expected or solicited. Phishing emails are often

at the root of most breaches and are becoming more difficult to recognize. Educating employees will help you to create a culture of security throughout your organization.

- **Establish internal cyber security policies.** This could include mandating stronger passwords, limiting access to sensitive patient data to relevant staff members, and backing up data. Consult with your IT manager to set workable parameters for your practice.

- **Increase password security.** Possibly the best security measure is to choose a strong password. Strong passwords often require staff members to change their passwords every six months and to use a combination of upper- and lower-case letters, numbers, and special characters. Instruct staff not to share passwords or have one password used by several employees for one system or account.

- **Review and audit your cyber security regularly.** Conduct an objective evaluation of your current cyber security controls and tools with your IT manager on a regular basis. Consider conducting an audit every six months, or at least every year.

- **Create a breach response plan.** If a breach does occur, be prepared. Have a breach response plan in place that assigns roles to staff members to help you keep your practice open.

  These roles could include a communication leader to manage media inquiries or to alert the media. The person in this role could also communicate to patients, vendors, or other clients about the breach. You may also select a documentation leader to document the timeline of the breach response, including what actions were taken and when. This can help you when conducting IT forensics or an audit.

  Make sure your staff is fully educated about their roles in the event of a breach. These roles could include reaching out to external IT experts for a solution or assigning someone to coordinate with TMLT regarding your cyber security coverage. Conduct a drill that tests your response plan. Identify and address any gaps in the plan or employee questions.

For more information on how to reduce your risk of a cyber breach and associated costs, please contact TMLT's Cyber Consulting Services at consultingwebmail@tmlt.org. TMLT cyber resources are also available online at https://hub.tmlt.org/cyber.

SOURCES

1. Goedert, J. CIOs and CISOs work together as attack threats grow. Health Data Management, January 31, 2018. Available at https://www.healthdatamanagement.com/news/cios-and-cisos-working-together-as-attack-threats-grow. Accessed May 1, 2018.
2. Ragan. S. Customers describe the impact of the Allscripts ransomware attack. CSO. April 17, 2018. Available at https://www.csoonline.com/article/3262168/ransomware/customers-describe-the-impact-of-the-allscripts-ransomware-attack.html. Accessed April 27, 2018.
3. 4 in 5 Physicians Had a Cyberattack in Their Practices, Says Survey. American Medical Association. December 12, 2017. Available at https://www.ama-assn.org/4-5-physicians-had-cyberattack-their-practices-says-survey. Accessed April 30, 2018.
4. Cooper, C. What is the cost of a breach? AT&T Business. October 24, 2017. Available at https://www.business.att.com/learn/secure-networking/what-is-the-cost-of-a-breach.html. Accessed April 30, 2018.
5. Maynard, T., Ng, G. Counting the cost - cyber exposure decoded. Emerging risks report 2017. Technology. Lloyd's. Available at https://cyberpolicymagazine.com/images/pdf-downloads/counting_the_cost_cyber_attack.pdf. Accessed May 1, 2018
6. Spitzer, J. The cost of a data breach in healthcare averages $717k: 5 report findings. April 6, 2018. Becker's Health IT & CIO Report. Available at https://www.beckershospitalreview.com/cybersecurity/the-cost-of-a-data-breach-in-healthcare-averages-717k-5-report-findings.html. Accessed May 24, 2018.
7. Cloud Down: Impacts on the U.S. Economy. Emerging Risk Report 2018 Technology. Lloyd's. Available for download at https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/cloud-down. Accessed April 30, 2018.

John Southrey can be reached at john-southrey@tmlt.org.

Wayne Wenske can be reached at wayne-wenske@tmlt.org.