ENVIRONMENT of CARE LEADER

Safety | Security | Emergency Management | Accreditation Success

May 22, 2017 | Vol. 22, No. 11

Security

Review cybersecurity plans now after hackers take hospital IT hostage

Use the recent international ransomware attack on hospitals and businesses to argue for more resources if you need them to ensure you can protect your facility from a costly shutdown — and a breach of patient information that could spell even more trouble down the road.

As HHS' Office of Civil Rights (OCR) has stepped up its HIPAA enforcement in the last few years, the last few months have also seen closer scrutiny of how prepared health care organizations (HCOs) are to deal with a cybersecurity attack, notes attorney and certified information privacy professional Alisa Chestler, chair of

*(see **Security**, p. 5)*

Ask the Expert

Develop easy labeling of chemicals on biohazard transport carts to aid staff

Question: *Concerning labeling of biohazard containers for endoscopy and the operating room. For the operating room, we currently spray gel on the instruments and place them in an enclosed case cart to send to the decontamination area. Will the labeling of the case cart for spray gel be something The Joint Commission looks at, as well as endo labeling of their hazardous containers?*

*(see **Ask the Expert**, p. 6)*

IN THIS ISSUE

Security

Ask the Expert

Life safety

What's wrong with this picture?

Environment of Care Leader | Toll-free: 1-855-CALL-DH1 | www.decisionhealth.com
Two Washingtonian Center | 9737 Washingtonian Blvd., Ste. 502 | Gaithersburg, MD 20878-7364

Security

Follow these tips for steps to take in wake of recent ransomware attacks

Use these tips to look at your own resources and assess your cybersecurity plan in the wake of the WannaCry attack *(see p. 1)*. These tips are from attorney and certified information privacy professional Alisa Chestler, chair of the Data Protection, Privacy and Cybersecurity Team for the Baker Donelson law firm in Nashville, Tenn., and Washington, D.C., and Frank Ruelas, a consultant and principal of HIPAA College in Arizona.

- **Communicate.** Prepare and send an alert for staff regarding their roles in preventing such attacks on your networks, says Chestler, who sent similar advice to her clients as well. Remind staff to be on the lookout for phishing scams in which hackers try to get employees to open infected emails, and report such scams to your organizations information technology help desk immediately if they are making it through your spam filters.

Also, remind employees that very few emails contain a true "emergency." Even if an email appears to be from a known source, everyone should be thoughtful when opening email attachments, says Chestler. And make sure employees know how to get to your IT help desk 24 hours a day, 7 days a week because system incidents are not limited to a 9-5 workday, Chestler advises.

"Many organizations try to keep their users aware of ongoing threats," notes Ruelas. "Many do so by sending out security reminders. However, often users will become desensitized to these reminders over time. This is why a 'flash' type of announcement by email and also by voice mail [many systems allow for messages to be sent by an administrator to all voicemail boxes] to alert people about this current threat may have been useful once it was known."

Afterward, organizations should use sensational attacks such as this to relate to employees why the routine security awareness reminders are sent out. "This can help revitalize people's interest and commitment to being watchful on messaging related to computer security," observes Ruelas.

- **Review your incident response plan.** Ensure communication lines between management, key IT personnel and legal counsel are open and ready to implement your cybersecurity incident response plan, says Chestler. Make sure the plan specifically anticipates a ransomware attack. It should also be in writing. Documented incident response plans are an expected compliance obligation for all organizations "regardless of the size, industry or kind of information maintained by the systems," notes Chestler in her advice to clients.

That includes making note of training and other steps taken as part of your incident prevention and response plan. Because if you do have a breach, the first question the government is going to ask is "did you do everything you could do" to prevent or mitigate it, says Chestler. "You need to have pretty robust documentation to show that."

Subscriber Information ▸ Have questions on a story? Call or email us.

Environment of Care Leader is published 24 times each year by DecisionHealth, LLC. Copyright 2017.

Have questions on a story? Call toll-free: **1-855-CALL-DH1**

President:
Elizabeth Petersen,
1-800-727-5257, x3432
EPetersen@blr.com

Vice President:
Tonya Nevin, x6036
tnevin@decisionhealth.com

Content Manager:
Jay Kumar, 978-624-4560
jkumar@blr.com

Editor:
A.J. Plunkett, x6001
aplunkett@decisionhealth.com

Join our DecisionHealth — Medical Practice & Hospital community!
www.facebook.com/DecisionHealthMP
www.twitter.com/DH_MedPractice
www.linkedin.com/groups/4048762

DecisionHealth Pledge of Independence: DecisionHealth's *Environment of Care Leader* works for only you, the provider. We are not affiliated with any special interest groups, nor owned by any entity with a conflicting stake in the health care industry. For nearly three decades, we've been independently watching out for the financial health of health care providers, and we'll be there for you and your peers for decades to come.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered and is NOT intended to be used as a substitute for legal advice. It is published with the understanding that the publisher is not engaged in rendering legal, accounting or other professional services. If legal advice or other expert assistance is required, the service of a competent professional should be sought.

SUBSCRIPTIONS: $447/year for 24 issues. For questions about newsletter delivery and account status, call toll-free 1-855-CALL-DH1 or email *customer@decisionhealth.com*.

ELECTRONIC VERSION: Don't want to wait for snail mail? Sign up for your free e-version of *ECL*. Just email *customer@decisionhealth.com* and tell us to add your email address to your subscription; include your account #, which you'll find just above your name and address on your paper newsletter. You will continue to receive the hard copy version in the mail.

FREE LISTSERV: ECL Talk is a free chat group where you can get advice from your peers and share your experience on daily challenges such as unannounced surveys, Life Safety Code, safety, security and more. To sign up, visit: *www.decisionhealth.com/ecl-enroll*.

MULTIPLE COPIES, SITE LICENSES AND REPRINTS: Could more than one person at your company benefit from a subscription to *Environment of Care Leader*? To request permission to make photocopy reprints of *Environment of Care* articles, call 1-855-CALL-DH1 or email customer service at *customer@decisionhealth.com*. Also ask about our copyright waiver, multiple copy and site license programs by calling the same number.

WARNING: Copyright violations will be prosecuted. *Environment of Care Leader* shares 10% of the net proceeds of settlements or jury awards with individuals who provide essential evidence of illegal photocopying or electronic redistribution. To report violations contact Brad Forrister at 1-800-727-5257 x8041 or email *bforrister@blr.com*.

- **Maintain good patch management practices.** Thousands of organizations were immune to this strain of ransomware because they were up-to-date with their patches, reminds Chestler. Leadership should ask whether critical patches are up to date. If they are not, initiate a plan to get your programs as current as possible.

"Patch management is a scalable process," says Ruelas. "Often the main decision on patch management is the business decision on when to install a patch. One overriding factor is to decide when to install a patch so as to minimize the impact on workflows and to minimize the number of users that may be affected."

- **Use this as an opportunity.** Management, legal and IT security can no longer keep "kicking the can" when it comes to information security, says Chestler. "Whether the systems include information on trade secrets or personal information of individuals (including employees), or the systems just keep the machinery up and running, computer systems and programs are the lifeblood of an organization. Knowing your compliance and contractual obligations before an event is critical," she says.

"This is also a good opportunity to revisit some prior decisions. For example, many organizations continue to delay implementing multi-factor authentication."

Multi-factor authentication goes beyond requiring login credentials for EHR or other networked systems. Sometimes it is a secondary fingerprint access system, an access code that is texted or emailed to the individual upon login or a key fob or token that regularly generates an access code for input before allowing system access.

There are a variety of reasons hospitals and other organizations avoid multi-factor authentication, including employee morale, observes Chestler. A doctor may insist that it is just too much added time in an already busy day. However, "this tool is widely becoming the most important information security protocol."

"If it costs you more than five or 10 minutes a day, I'd be surprised," Chestler notes. "Most people spend at least that much time in their work day on Facebook" or other social media.

The delay to use a multi-factor access authentication is "infinitesimal to the effect of a breach," she adds.

Similarly, this may also be the time to ask leadership for more IT or training resources. Run the cost of those against the cost of a shutdown or government investigation into a breach of PHI.

If resources remain a concern, consider teaming up with partner organizations and business associates to share security assessment measures, recommends Chestler.

- **Update your security risk assessment.** Required by HIPAA regulations, the security risk assessment should be reviewed at least annually or whenever there is a major change in the IT system, says Chestler. Also keep in mind when you did the risk assessment. Five years ago the focus was less on ransomware and more on laptop encryption, notes Chestler. Do another security risk analysis "with the current landscape in mind."

- **Review your cybersecurity coverage.** Make sure your insurance covers what you think it does, says Chestler and other experts. "You need to have cyber liability coverage," she says. "You've got to be able to hire the knowledgeable forensic investigator to deal with this," because most organizations are not large enough to have someone on staff to handle it.

Your insurance policy should cover breach response, including the investigation of what's happening and the experts to advise you how to handle it. While you can and should notify the FBI to help in the response, they are going to be able to help you in the moment, says Chestler. But "they are not going to write you up a report for a regulatory requirement," which you might need later to show you met your responsibilities toward attempts to protect PHI.

- **Test and train on your incident response plan.** Besides training users on EHR or other technology system security measures, says Ruelas, "hospitals should also consider either actual or table top exercises mimicking a cybersecurity threat such as malware. This may provide an organization with genuine insight on how well, or not, it is positioned to respond to a ransomware attack that happens at time zero."

Ensure the test can answer some basic questions on how your organization responds to such an attack, advises Ruelas.

"Would the response resemble an incident response exercise or would it be unorganized and chaotic? How long was the last incremental or full system backup? How long would it take to restore recoverable files? Are the downtime procedures adequate to fill the lack of system access during an attack? These are some of the questions that organizations need to ask and get answers to now and not in the times of high stress, high anxiety, and high stakes that often result during an actual attack."

— A.J. Plunkett (aplunkett@decisionhealth.com) and Brian T. Ward (bward@hcpro.com)

Security

(continued from p. 1)

the Data Protection, Privacy and Cybersecurity Team for the Baker Donelson law firm in Nashville, Tenn., and Washington, D.C.

OCR was so concerned about ransomware, it issued an alert in July 2016 to make sure hospitals and other HCOs understand that the enforcement agency may consider such an attack a reportable breach of protected health information (PHI), depending on the circumstances *(ECL 8/29/16)*.

In addition, failures to adequately protect your electronic health records (EHR) could be seen by CMS and The Joint Commission (TJC) as failures in protecting patient information and even patient safety.

One EHR provider recently sent out a warning about a security patch that elevated the problem to the level of patient safety, not just PHI security. *(See article on eClinicalWorks warning, p. 4.)*

CMS issued guidance to its surveyors earlier this year to counsel hospitals on best practices to boost their cybersecurity, signaling that such protections were expected to maintain accreditation *(ECL 2/27/17)*.

Attack was international

The recent attack came to light on Friday, May 12 when Britain's National Health Service began reporting that it was halting medical procedures because of a computer shutdown.

Before long, media reports were noting that a ransomware virus dubbed WannaCry was spreading, eventually locking thousands of computers in as many as 150 countries. The hackers reportedly were threatening to delete files unless they were paid a ransom, which some reports said was as little as $300 in the digital currency of bitcoins.

U.S. health care organizations and businesses avoided being part of the massive attack, which exploited a software problem for which Microsoft had issued a patch in March. Industry observers speculated that most users in the United States used the patch and avoided infection. Ransomware often infects a computer system through email, if an employee clicks on a link or opens an attachment that contains the virus or malware.

While employees should be trained and reminded not to open attachments or click on links in emails from someone they don't recognize, experts say that hackers have also become proficient at sending emails that appear to be from someone the person knows.

Patch management critical

The fact that so many hospitals and other HCOs outside the U.S. were compromised, says Frank Ruelas, a consultant and principal of HIPAA College, points to a larger issue — "poor or nonexistent patch management."

Patch management, "where system administrators make it a point to get the latest software updates that fix 'bugs' or security flaws, is a long standing practice that most if not all well run IT [information technology] departments should have as a 'must do' in the standard operating procedures," says Ruelas. "Though a successful attack is primarily a function of a computer user clicking on a link that launches malware, the fact that many computers were compromised also speaks to the fact that many organizations did not install this particular patch."

Ransomware a business now?

In alerts that went out that Friday and continued through Monday and Tuesday, HHS and other enforcement agencies encouraged HCOs and businesses to take precautions, but recommended not paying any ransom and to notify the FBI immediately if an attack was detected.

While the WannaCry attackers reportedly got only about $20,000 in ransom worldwide, hospitals and other HCOs in the United States have faced the choice of whether to pay or not in ransomware attacks for the last few years. Some have paid thousands to unlock their systems, while others have not *(ECL 2/29/16)*.

Hospitals should be prepared to face that question should they become victim to an attack. "I'm not saying whether you should or shouldn't pay the ransom," notes Chestler, saying that the question at that point becomes, "What's your plan?"

First you have to answer, "do you have an adequate backup system to get up and running in a timely fashion, and can you do so with accuracy and integrity?" asks Chestler.

Remember that for hackers, "ransomware is a business now," she says. Paying the ransom may speed your recovery because the perpetrators will release your computer systems — if they don't, word will get around and they will no longer be able to collect ransom, she explains. But paying a ransom could encourage further attacks.

Whatever you choose, do it quickly. Chestler offered the story of a small law firm in Rhode Island that faced a ransomware attack and chose not to pay, assuming its cybersecurity insurance would cover the cost of the business interruption.

It didn't. By the time the firm tried to go back to the hackers to pay the ransom, it was too late. The attackers had discarded the key to unlock the systems and moved on.

Exciting changes are coming!

DecisionHealth, which publishes **Environment of Care Leader,** and HCPro are now part of the same family!

In the coming months, **Environment of Care Leader** will transition to a more frequent and robust online publishing model by combining with **Briefings on Hospital Safety,** the flagship publication of HCPro's **Hospital Safety Center** (*www.hospitalsafetycenter.com*). As an existing **Environment of Care Leader** subscriber, you will be granted full membership to **Hospital Safety Center.** This will create a single source for all your compliance and healthcare safety news, tools, and best-practice strategies. Each week, we will release new articles on **Hospital Safety Center.** At the end of the month, we'll roll the weekly articles into a digital issue of **Briefings on Hospital Safety.** As a member, you can continue to download and print high-quality PDFs of the current digital issue, as well as several years of back issues of both **Environment of Care Leader** and **Briefings on Hospital Safety.**

Hospital Safety Center members also receive monthly security improvement strategies, advice, and analysis through **Healthcare Security Alert Online** and breaking news on safety-related incidents at hospitals around the country, as well as the latest regulatory updates through the weekly e-newsletter **Hospital Safety Insider.** Plus, members can read up on the latest hospital safety issues on **Mac's Safety Space,** a popular blog written by HCPro's hospital safety expert Steve MacArthur.

We're looking forward to delivering your compliance and safety guidance in a more timely, efficient, and convenient manner. Stay tuned in the coming weeks for more information on these exciting changes.

Sincerely,
Jay Kumar
Associate Product Manager, Accreditation and Safety
HCPro, an H3.Group Brand

Review resources now

Dealing with the actual attack is only part of the problem, says Chestler and others. Afterward, you may also face scrutiny over a breach in PHI. Remember that not only are federal investigators from OCR paying attention, but your state regulators will be as well. Almost all states have breach of privacy information regulations that are as strong or stronger than federal requirements, Chestler warns.

And if patient safety is compromised or threatened, you also could face CMS and TJC inquiry. *(For tips on response in wake of the WannaCry attack, see p. 2.)*

Review the resources and alerts sent out by HHS and other government agencies, and take advantage of other resources as well. For instance, the American Hospital Association has set up a public-access webpage with information as well as links to members-only webinars and other training programs on cybersecurity. *(For links, see Resources below.) — A.J. Plunkett (aplunkett@decisionhealth.com) and Brian T. Ward (bward@hcpro.com)*

Resources:

- HHS Update: International Cyber Threat to Healthcare Organizations: *https://asprtracie.hhs.gov/documents/newsfiles/NEWS_05_13_2017_08_17_11.pdf*
- US-CERT National Cyber Awareness System webpage at: *https://www.us-cert.gov/ncas*
- FBI FLASH alert — Indicators Associated With WannaCry Ransomware: *https://content.govdelivery.com/attachments/USDHSCIKR/2017/05/13/file_attachments/816377/FLASH_WannaCry_FINAL.PDF*
- AHA cybersecurity advisory page: *http://tinyurl.com/AHA-cybersecurity*

Ask the Expert

(continued from p. 1)

Answer: Yes, says Jennifer Cowel, a former nurse surveyor and executive at The Joint Commission (TJC) and president of Patton Healthcare Consulting in Naperville, Ill.

"The Joint Commission will expect that, at minimum, the case cart or carrying case that you are using to transport dirty instruments or dirty scopes from the procedure room to the decontamination area is clearly labeled with the biohazard label."

Cowel notes that case carts hospitals use fulfill many of the requirements outlined in ANSI/AAMI ST79, "Comprehensive guide to steam sterilization and sterility assurance in health care facilities," which is the go to evidence-based guidelines for handling such medical devices.