10 Things Clinicians Need to Know About Healthcare Cyberattacks

Paul Rizzoli

Assistant Professor, Harvard Medical School and Clinical Director, John R. Graham Headache Center, Department of Neurology, at Brigham and Women's Faulkner Hospital, Boston, Massachusetts, USA

e-mail: prizzoli@bwh.harvard.edu

Abstract: The threat of cyberattacks on healthcare systems is increasing. Individual providers should be aware of potential weaknesses in their systems and should begin immediately to look for ways they can help to minimize the risks of a potentially devastating attack upon their healthcare system. Examples of potential threats are reviewed along with suggested solutions. Going forward we will all need to become more educated in order to help prevent such attacks.

Keywords: Cybersecurity; Healthcare_system; Electronic_medical_record (EMR); Medical Informatics

Threat of cyberattacks on healthcare systems

October 28, 2020 was a bad day for healthcare cybersecurity. Reports emerged of cyberattacks directed at hospital systems in three US states, triggering a joint alert by three federal agencies: the Federal Bureau of Investigation, Department of Homeland Security, and the Department of Health and Human Services (1). The impact of these attacks was reportedly severe, although the consequences of cybercrime involving health systems are often kept quiet.

It is certain that more attacks of different kinds are coming. A recent attack at a North East university hospital (2) system disabled the electronic medical record system for weeks, forcing providers back to paper records and prescriptions, with limited access to old records, and widespread disruption of patient care. One of our Headache Medicine colleagues experienced this firsthand. There was a sudden loss not only of the electronic medical record but of radiology, prescribing and ordering systems, phone and e-mail. Imagine calling the referring provider to request your last note be faxed BACK to you so you could pick up where you left off and see your patient in follow-up, recording vital signs, history and exam features on paper and handing out written instructions. Also think about how difficult it would have been to set up an MRI, an infusion or to get approval for Botox or a CGRP MAB. Also, since the specialist's work files were on the hospital server, our colleague was without access to all personal work files. The disruption occurred without notice and lasted over a month. What can individual clinicians do to help protect our own institutions, our patients, and ourselves?

The members of the American Headache Society Informatics Special Interest Group crowd-sourced a list of common cyberthreats and related issues and behaviors. In the Table, we provide examples and scenarios of both threats and issues related to cybersecurity and then suggest some best practices.

Though the recommendations (Table 1) focus inward on the actions of the individual provider, there may also be, at times, a need for us to look around and advocate for both better work conditions and better security. As with the password issue mentioned in the table, employers may at times be seen to go in the wrong direction in the name of security and we may wish to point this out. One scare tactic by employers highlighted in a recent WSJ article (5) should be mentioned. This is the practice by some health systems of sending out fake phishing e-mails to employees in an attempt to both trick them and alert them to the security danger. Our system does this routinely. Some organizations however have carried this to an extreme by publicly shaming or fining those who mistakenly click on an inappropriate link. Not only was this practice seen as anxiety-provoking and morale-destroying for employees but, of critical importance, was shown to be ultimately ineffective. One alternative creative solution had employees working together as teams to identify suspicious e-mails and then notifying the rest of the system to be aware. The result was both improved security and improved morale.

Conclusion

Further cyberattacks are coming to healthcare. Any one of us could be victim at a moment’s notice. We should all be committed to finding creative solutions in order to protect our patients, our institutions and ourselves.

Table 1. Ten Things Headache Medicine Specialists Need to Know About Healthcare Cyberattack

	Scenario	What's the problem?	Best practice solution
1.	You receive this email said to be from AHS that though plausible is atypical and looks like: *"Important: Your Password will expire in 1 days.* *Dear AHS member,* *This email is means to inform you that your AHS password will expire in 24 hour.* *Please follow the link below to update your password."*	This is a practice known as "phishing," the fraudulent practice of sending emails purporting to be from reputable companies or organizations to attempt to trick users into revealing personal information or to allow a point of entry into the network. Often the email will contain grammatical errors. It will direct you to click on links or files that will upload the virus.	Educating yourself and colleagues or employees about "phishing" is the most important step towards combating it. Users should not click on any attachments they have not verified. If sent a file to open, your first action should be to call the sender and verify that they did indeed send over a document. Never use any numbers or contact information contained in an email; instead look up the contact information separately.
2.	You receive this e-mail and since you train Headache Medicine fellows this does not seem completely unreasonable: *Subject: 2020 Fellow Evaluation* *From: billygoodwell30@gmail.com* *To: user@mansgrtsthosp.edu* *2020 Fellow Evaluation* *Fill out Form* *Hxxps://docs.google.com/forms/d/e/1FellowA1IdDd4_kVi24_k*	Another example of phishing. This is adapted from: https://security.berkeley.edu/news/phishing-example-2020-faculty-evaluation accessed 1/9/21 Best practice for phishing emails which often contain incorrect addresses, grammatical errors, as above, make urgent requests or contain suspicious links: If you don't know the sender, or the email address is fake or if you don't recognize the link it is likely malicious. Reject it and DON'T click on the link. Attempt to contact the sender separately by phone to verify or report the e-mail as phishing or spam to IT.	
3.	It's easy, convenient and it's always nearby; it's your work email: John/JaneDoe@Man'sBestUniversity.edu . Over time you notice junk mail that may relate to the times you used it to order takeout, rent skis, get a quote for home services or a thousand other things.	For many of us, our work e-mail has become our identity, used for everything and monitored constantly. Some keep a separate, private e-mail but monitor it on their work machine. Topics and discussions in private e-mails may be inherently more diverse and insecure than those seen in work e-mails.	Best to keep a separate, private e-mail address firewalled from your work system. Keeping this separate and off of work machines should make it more difficult for malware to enter the system through insecure channels. Notwithstanding the inconvenience, there are other reasons to consider maintaining your own private e-mail account outside of the work system, not the least of which is that work e-mails are ultimately not your property and may be accessed by work officials under certain circumstances.
4.	There is a particularly interesting discussion happening on your Facebook migraine group and it is easier for you to keep up with it if you keep Facebook open on you work desktop. Besides, this way you can follow your brother's travel photos as they are posted.	Much malware entry can be traced to the use of personal email or social media and running these programs on your work computer can be very dangerous because these programs are common entry points for hackers and can expose the healthcare network to security risk.	Best to avoid the use of these social media programs on work systems as these cuts down on possible entry points and helps protect the integrity of the work system. However, cutting employees off entirely from their private life for the entire workday may seem unreasonably restrictive and impractical. For a possible solution, see scenario #4.

Table 1. Continued

	Scenario	What's the problem?	Best practice solution
5.	During a busy day in clinic, all computer systems start to run slowly. The clinic manager suspects perhaps a network intrusion and notifies IT. They trace the problem to one location and find you tweeting intently about an issue you hold dear, with your device hooked up to the network letting in malware. May sound far-fetched but intrusions can start like this.	To reiterate from scenario #3, the use of social media programs like Facebook, Twitter and LinkedIn has exploded in recent years. Clearly there are very legitimate work uses for social media. Nonetheless there are significant security issues created by their use in the work setting since a large number of viruses and scams seem to originate on social media. Your organization may also have restrictions on the use of social media programs on their network so be aware.	Best to familiarize yourself with all security policies for your organization. One possible solution that seemed common in the tech world is the use of a private phone or laptop, certified by work, if necessary, and used on the "guest" network at work completely outside of and separate from work machines. These could run your private e-mail and social media programs keeping you connected and the healthcare network safe.
6.	You were not paying attention and missed the multiple warnings to change your password before a certain date and now your work computer is locked and unavailable for your use. You finally get in and get your password updated using a trusty variation of your usual password: kittycat123.	We all tend to fall into bad password habits such as creating weak passwords and using them again and again. Current healthcare system rules requiring frequent password changes may only foster sloppy habits and, in the end, actually reduce security. At the same time attackers are becoming more and more sophisticated at determining passwords generated by users. Once malware has provided attackers with access to a machine, they may locate lists of old passwords. With the temptation great for users to reuse passwords with minor changes, attackers can easily guess current passwords.	This issue is in need of a best practice. A secure password should be both long and complex, exactly the opposite of what you could easily remember and enter quickly. It should preferably be random and auto-generated (2).This requires use of a password manager program to save and provide the password each time it is needed (3). Currently however, these don't work with medical record systems. Thus, given the need to enter a password multiple times a day, a 20-character complex password is not practical, and this remains a security weakness. We are thus currently left on our own to generate a reasonably more lengthy and complex password than kittycat123.
7.	It is more and more common these days, when signing into a website, to encounter a two-step process wherein you are instructed to go to your phone to obtain a separate code sent there and put that into a box on the site before entry is granted.	This electronic method of authentication offers an extra layer of security and though it is an extra step for the user is very difficult for attackers to overcome. To gain access to a site, the user is required to provide two or more pieces of evidence that only the user knows, something he/she knows or has, like a code or password, or something she/he is, like a fingerprint.	Best Practice: Yes, this is an extra step. No, don't become frustrated. Be happy when you see this since it really increases your security. It may be offered by banks or similar institutions when you create an account, for example, but you need not select to use it for your account. When offered by your IT system as an option, multifactor authentication should always be employed. Mobile phone-generated codes have made the process more seamless.

Table 1. Continued

	Scenario	What's the problem?	Best practice solution
8.	Your entire healthcare network has been shut down and locked after an attack. You sit looking at your blank desktop screen as it slowly dawns on you that the only copy of your PowerPoint Presentation for Grand Rounds next week is on that desktop. So is the updated spreadsheet of data for the paper you are writing, the letter of recommendation that was due last week, the updates to your CV….	If your work system is compromised you may either lose temporary access to, or never again see, all of the academic work, correspondence, CVs and protocols that you have stored on that system. This could happen at a moment's notice and could prove devastating.	All of your personal work should be stored or backed up off of the work system. There are a number of options, as there are at home, depending on preferences and risk tolerance. Our organization provides employees with access to Dropbox that can be configured for different layers of backup to the cloud either automatically or manually. Backing up personal documents to a portable drive allows you to access and work on them in multiple locations, keeping a copy on the work system in case the drive becomes inoperable or lost. Critical documents may be e-mailed to yourself to preserve yet another copy. The overall best practice is to maintain an awareness of the impact of the loss of each document in your control and to act accordingly to maximize its protection.
9.	Ever look at the App Store icon on your private computer or phone? There is often a red dot containing a number in the upper corner of the icon. Many people either don't know or care what it means; it indicates how many application updates are waiting for installation on your device	Most applications are updated periodically, usually bug fixes but often security updates as well, and notification is sent to the owner to install the update for continued safe and smooth running of the application. It stands to reason that you are most protected when the applications you use are current and up to date, but like many computer maintenance issues, updates often go unattended.	Though you may have little control over work application updates, it is good practice to keep private equipment running optimally by following recommendations for routine updates of operating systems, installed programs and antivirus software.
10.	You are starting your afternoon in the clinic. The medical record seems to be running a bit slowly, a minor annoyance you think. Then you try to send a patient letter and the system hangs. You restart and try to write a prescription and the electronic medical record shuts down. You check and others are experiencing the same problem. When you return to log back in, your entire computer is locked.	It does not seem real until it hits your clinic, your computer and your files, and then it is all too real and also too late. Like a hurricane, a cyberattack is a disaster that might occur but is hard to predict, difficult to imagine and the potential threat is easy to ignore. The recent warnings however suggest that the threat is very real, and preparation is urgently needed systemwide.	In addition to the best practices outlined above we can also be leaders in our professional societies, such as the American Headache Society, and in our communities supporting the call for legislative and other action to improve cyber protection. Patients' lives literally depend on it.

References

1. Vole D, McMillan R. Hospitals Hit with Malware Attacks. 10-30-20. Wall Street Journal <https://www.wsj.com/articles/hackers-hit-hospitals-in-disruptive-ransomware-attack-11603992735> (accessed 10/29/2020)
2. Barry E, Perlroth N. Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack. 11/26/20. <https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html> (accessed 12/10/20)
3. Brecht D. Password Security: Complexity vs Length. 9-8-19. Infosec. <https://resources.infosecinstitute.com/topic/password-security-complexity-vs-length/> (accessed 11/24/2020)
4. Rubenking NJ, Moore B. The Best Password Managers for 2021. 12-21-20. PC Magazine. <https://www.pcmag.com/picks/the-best-password-managers> (accessed 11/25/20)
5. Kruse CS, Smith B, et Al. Security Techniques for the Electronic Health Records J Med Syst. 2017; 41(8): 127. Published online 2017 Jul 21.
6. Renaud K. Why Companies Should Stop Scaring Employees About Cybersecurity. 12-7-20. Wall Street Journal. <https://www.wsj.com/articles/why-companies-should-stop-scaring-employees-about-cybersecurity-11607364000?reflink=desktopwebshare_permalink> (accessed 12/24/20)

Contributors:

The authors would like to acknowledge Eric Darsey, Cyber Command Center Technician at American Well Corporation and Joan Goodchild, veteran journalist covering cyber security for more than a decade and founder of Cyber Savvy Media for providing background information for this article and members of the Informatics Special Interest Section of the American Headache Society who were crowdsourced for their comments on the topic.