MEDITECH EXPANSE

Strategies to Protect Your Organization from Cybersecurity Threats

According to *Becker's Health IT & CIO Review*, maintaining the privacy and integrity of confidential data while also reducing security risks are among CIOs' top IT concerns. Viruses, ransomware, malware, phishing schemes, and other cybersecurity threats can all wreak havoc on your network, devices, and data which has a detrimental impact on your staff's ability to care for patients.

As a leading EHR provider, we've encountered many of these threats and assisted our customers to recover. We've seen the impact they've had both on our customers and those using another EHR. To help mitigate this threat, we've compiled a list of industry-standard practices your organization can follow to protect the security of your data, and more importantly, the privacy, health, and safety of those under your care.

Enlist the C-Level

Cybersecurity requires a team approach. All teams need to work to prepare for a cyber incident because we all have a role to play in protecting the organization. We all need to prepare so that when the systems are down, we can still perform our mission. Cybersecurity is a patient safety issue and thus requires the attention of everyone.

Sometimes people will ask "Who will save us?" There is this view that cybersecurity professionals will rush in and save the day. The reality is that we all play a role, and the question we should be asking is "Who will help us?"

Security professionals are here to assist, but we all work together as a team. We must never lose sight of the fact that the organization does not exist for the sake of security. Security exists to serve the needs of that organization as they perform their core mission.

In particular, healthcare leadership must take an active role. While CIOs and CISOs and other IT professionals are deeply involved in this struggle, we need advocacy from CEOs, COOs, CMIOs, and other healthcare leaders. Cybersecurity is not purely a technical problem, and thus technology alone will not solve it. Additionally, all leaders need a clearer understanding and appreciation for the digital infrastructure that supports their organizations.

If a hospital's physical infrastructure were compromised — perhaps the foundation is crumbling — it would get immediate attention. We all understand how serious that is. The digital infrastructure is not so well understood by everyone.

> *"Don't leave the details to others. Active, hands-on engagement by the executive team and the board is required.* ***The risk is existential.*** *Nothing is more important. Your involvement will produce better results as well as make sure the whole organization understands just how important the issue is."*
> — Former CEO of Visa Charles Scharf *(Forward from "Navigating the Digital Age")*

Now is the time to involve hospital leadership and to engage all staff. To do this, security leadership must understand the organization's mission and support the organization — finding ways to do things while keeping them secure — rather than being an obstacle to progress. Security leaders must take the time to do more than simply educate others — they must work to help them *understand* these issues. They must engage with everyone regularly.

Update and Patch Your Systems

Old versions of Windows Server (currently 2008 R2 and earlier) should be updated to a newer version. Patches should be applied in a timely manner for all versions. Hackers frequently exploit vulnerabilities that have already been fixed by the software developer. Typically they exploit systems that have not taken the updates to address vulnerabilities that have already been fixed for a year or more.

Client operating systems and all other software, browsers, or plug-ins need to be kept up to date and patched as well. This is critical for anything that is externally facing. Google, Shodan, and other tools make it easier than ever for attackers to find vulnerable systems.

Protect Your Clients

Clients (end-user devices) are most frequently how the ransomware gets a foothold into a network. A user may download an infected file or click on a link to a malicious site. Once the malware executes on the client device it will not only encrypt files on the client but look for file shares and mapped drives as well. Most often this has been how files on servers have been encrypted — via file shares.

In addition to updating and patching client software, you should follow these best practices for client devices:

- Ensure your antivirus software is running and has the latest signatures.
- Uninstall unused software, because attackers may be able to exploit a vulnerability.
- Remove insecure browser plug-ins.
- Install website popup blockers.
- Restrict privileges as much as possible without impacting functionality.
- Uninstall browser plug-ins that are unused, vulnerable, or of a questionable source.

Complement Your Network with the Right Technologies

While there is no "silver bullet," the right combination of technologies can play an important role in preventing attacks. For example, there are secure email gateways that prevent malware from gaining a foothold, even when the user clicks on the link or downloads a malicious file. Statistics show that even among the staff who have received regular security awareness training, there is a fair number that will still click on things they shouldn't. In light of the increasingly convincing phishing emails, it's not realistic to expect that we will ever prevent phishing 100%. This is where a technological solution can mitigate the risk.

Trustworthy Email

Perhaps you have already experienced this - after training and phishing your staff, they no longer trust anything. Staff may send you repeated messages asking “is this email legitimate?” While this is good that you have raised their awareness level, we need to consider what we can do to help them quickly identify trustworthy emails.

First of all, consider creating a set of standards for corporate emails. Every time we send out an email that says “click on this link for more details” we are undoing all of our work in educating them to hesitate before clicking. But we don’t want them to also suspect every email from us. We could provide a brief explanation about how to identify the current email as legitimate (hover over the link, examine the “from” field) or we could forego links altogether. Rather than sending them a link, ask them to navigate to your intranet page and tell them how to locate the page you would like them to read.

Second, work with your email solution to implement the following:

- **Spam Filtering** - Many email products come with this.
- **Scan Email Attachments** - Attachments are a major vector for malware.
- **Add a warning** to emails that originate from outside the organization.

We also want to prevent spoofing of our email domain. Not only does this benefit our internal staff, but it can prevent spammers from using our domain in attacks on other organizations. This can be accomplished through the use of SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). We can then move to implement DMARC (Domain-based Message Authentication, Reporting and Conformance) once SPF and DKIM are in place. The H-ISAC has challenged healthcare to adopt this immediately (https://h-isac.org/healthcare-best-practices-for-securing-email/) and it is now a requirement for all of the Federal Government (https://cyber.dhs.gov/bod/).

Run Antivirus; Keep it Up to Date

Antivirus (A/V) is not perfect protection by any means, but it’s widely acknowledged that it should be present. Make sure that A/V definitions are up to date. Consider a next-generation EDR (Endpoint Detection and Response) — while typically more costly, they are effective against the latest file-less malware threats which are missed by traditional A/V.

Backup Your Systems

Backups are essential. Healthcare organizations with well-tested and protected backups have been able to recover, and those with disaster recovery environments have been able to do so quickly. It is essential to have a plan for restoring user client devices as well. In some recent cases, thousands of client devices were encrypted and there was no way for users to access the MEDITECH EHR.

Know Your Network

This is not an easy task. But as Curtis Dukes[1], executive vice president & general manager of the Security Best Practices & Automation Group at CIS, put it: “How can you protect what you don’t know?” Not only should you understand the architecture of your network and its various segments and domains, but what kind of software users are downloading and installing on their work PCs. Are end users uploading information to DropBox, OneDrive, and other cloud services?

[1] https://www.cisecurity.org/about-us/leadership/curtis-w-dukes/

Eliminate file shares and mapped drives. These may be used to spread the infection to other machines. Make sure to carefully determine what the impact on functionality will be if you remove a File Share.

Lock Down Microsoft Word

Microsoft Word macros have been used to spread ransomware. Typically this has only affected end-user clients, not servers, but obviously, no one wants ransomware to gain any kind of foothold in the network from which to spread. Additionally, there may be some servers that have MS Word installed to generate reports. Staff education and proper configuration of MS Word are the solutions.

Use Strong Authentication

Passwords alone are not adequate for protecting email and critical work accounts. Cybercriminals are more effective than ever at phishing attacks, and it is quite easy for them to steal a password. Hence the need for additional "factors of authentication" — such things as RFID badges, authenticator apps, or a one-time password (typically received over the phone or via text).

Hack Yourself

Have a Penetration Tester actively attack your network. They will look for many of the things we've just mentioned using the same tools available to the hackers. Penetration Testers will not just look at your patching levels but will also have an eye out for misconfigured servers, vulnerable medical devices, poorly chosen passwords, default passwords that have not been reset, information about your organization exposed on social media, and much more.

For example, the individuals behind the SamSam malware exploited misconfigured JBoss installations. Even if the software was up to date, it did not matter — the problem was that there was essentially a back door left wide open by default.

Scan your systems from an external perspective as frequently as you possibly can. The most severe ransomware attacks of 2017 and 2018 have all involved servers which were accessible from the internet. Weak passwords and forgotten vendor support accounts allowed easy access for the attackers who then spread throughout the network and triggered the ransomware to start at an inconvenient time, usually on a holiday or weekend around midnight.

Establish and Communicate an Incident Response Strategy

Incident Response requires advanced planning. Who should coordinate the response? What criteria should be the guide in determining if a public statement should be made? Will there be a forensics team on retainer? The Incident Response team should have representation from the Executive Team, Legal, Public Relations, and other key divisions — it should not just be IT and Information Security. Such advanced planning will help you to determine whether or not the following should be the first steps you take if you find ransomware or other malware infection in your network:

- **Isolate** the affected machines immediately.
- **Contact your Cyber Insurance and/or Incident Response firm —** Often your cyber insurer will stipulate who you must use for incident response.
- **Determine the scope of the infection:** did it spread to other machines on the network?
- **Contact law enforcement**
    - In serious cases, call your local FBI Office directly (https://www.fbi.gov/contact-us/field)

- In minor cases, submit a complaint to www.ic3.gov — the FBI does review every submission, and even if you are not contacted, it provides useful information to them. It can help them to see the scope of the problem.

Educate Your Staff

Awareness is key. There are several strategies for making your Security Awareness training effective:

- **Make it interesting and relevant**
  - Tell stories — Include real-life examples.
  - Provide practical tips that they can apply in their personal life.
- **Provide regular reminders,** preferably in the form of a brief weekly post.
- **Provide a contact** that everyone can turn to when they have questions.
- **Build a culture of "see something, say something"™**
  - Encourage staff to speak up when they see something that is odd or suspicious
  - Provide a central contact for reporting
  - Don't berate or punish staff when they make a mistake; they are victims and we want them to come forward quickly.

For staff to prevent ransomware, they need to have an understanding of how it spreads. Don't just tell them "be cautious what you click on," but show real-life examples which illustrate just how well-made phishing emails can be. Explain how attackers can craft an email that looks legitimate but redirects them to a different webpage.

Ransomware — and other types of malware as well — generally enters a network in one of the following ways:

- **Malvertising**: A malicious advertisement placed on an otherwise reputable website. This occurred recently on the following prominent websites: MSN, BBC, the New York Times.
- **Watering Holes**: A popular webpage, such as Facebook, is compromised and used to spread malware. Recently a security organization's webpage was even used to spread malware.
- **Phishing Emails**: The email either directs the person to a malicious website or has an attached file (frequently a Word document or Adobe PDF).
- **Exploit Kits**: A set of software that is used to find vulnerabilities in systems and then to exploit them. Common exploit kits are delivered via "watering holes" or malicious websites.

Tips for Success

- Don't oversell; you will come across as "the paranoid security guy." Be realistic, and calmly explain the threats and risks.
- Many organizations will phish their employees and then require additional training when they fail. We must be careful not to make it appear as if they are being punished for their mistakes. Honestly, many phishing emails are extremely convincing. Treat staff as adults, and explain that it is easy to be tricked and it will take time to change our habits of clicking on anything that looks authentic. "Stop, Think, Connect." (https://www.stopthinkconnect.org/)
- Explain to staff that if a hacker has already taken over someone else's email account, they may respond to existing email threads and provide a link or attached file.

Stay Up to Date

We have mentioned the importance of staying "up to date" several times now, with regards to Software versions, A/V signatures, and so forth. It's also important to stay up to date with the latest news. At first, ransomware arrived mainly via phishing and only encrypted certain files. As time has progressed, some variants of ransomware are now spreading via malvertising and exploit kits. In the past, ransomware used to leave shadow copies and backup drives alone. Now it has been seen to encrypt shadow copies and to search out file shares and mapped drives (potentially these are backup drives) and encrypt those as well. Most recently, attackers are exploiting systems that are open to the internet and using that as a base for spreading throughout the entire network.

The FBI's InfraGard program (https://www.infragard.org/) is a way for you to interact directly with your local FBI and to gain access to intelligence about healthcare cybersecurity. InfraGard members can join the Cyber Health Working Group (CHWG) which provides a secure forum for discussion. The Health ISAC (H-ISAC - https://h-isac.org/) is another community worth considering. We urge all healthcare organizations to stay abreast of the latest developments through their preferred security sources or consultants. Two such resources we find valuable are US-CERT and CVE.

Resources

- Cybersecurity & Infrastructure Security Agency (CISA): https://us-cert.cisa.gov/
- KnowBe4 Blog: Ransomware Hostage Rescue Manual at https://blog.knowbe4.com
- No More Ransom! (https://www.nomoreransom.org/): A joint project between law enforcement and IT security companies, this website is a great resource on prevention, available decryption tools, and how to report crimes. There is also Crypto Sheriff, a page where you can upload files to find out if a solution is available for the strain of ransomware you're dealing with.
- Cybersecurity Collaborative Webinar: Practical Information for Healthcare Cybersecurity (Vimeo)
- MEDITECH Webinar: An Insider Look at Cybersecurity (registration required)
- Electronic Health Record Association (EHRA) response to Senator Mark Warner
- Cybersecurity at MITRE — CVEs, CWEs, CAPEC, ATT&CK®, MITRE Shield
- H-ISAC: Healthcare Best Practices for Securing Email
- Independent Security Evaluators: "Securing Hospitals" (PDF) — Well worth reading, this research study introduces the "Patient Health Attack Model."
- Cynergistek's 2018 Report on Cybersecurity Findings in Healthcare
- Fortified Health Security: 2021 Horizon Report
- Microsoft Local Administrator Password Solution (LAPS) — One simple technology which can be easily implemented and which will reduce your attack surface significantly.
- Current Threats: Ryuk, MAZE, Conti, "Living off the Land" (LotL)
- ACSC: Securing PowerShell in the Enterprise
- "Navigating the Digital Age" — The Definitive Cybersecurity Guide for Directors and Officers (free PDF). You may also obtain a second edition — which has entirely new content — from here.
- HHS: HIPAA Settlement Underscores the Vulnerability of Unpatched and Unsupported Software