Confronting Cyber Threats to Your Practice

BY SEAN HALL AND ADAM REBHUHN

How to prepare for—and respond to—a potential catastrophe

Cyberattacks can take place against any entity on any scale, striking both individuals and multinational companies with consequences big and small. As we have seen repeatedly, not even the largest companies with the most sophisticated security resources at their disposal are immune from security breaches.

The healthcare industry is particularly vulnerable to attack because medical practices typically house their most valuable data on the web. The severity of an attack and its impact on a practice can vary dramatically. Attacks can range from relatively benign actions, such as installing simple adware, to threatening a whole practice by compromising an entire network.

Even if you have not experienced a malicious cyberattack, it is critical to have a plan in place to prepare for the possibility of a security breach. Often something as simple as an employee opening a phishing email can escalate into a device compromise that can disrupt, delay, or shut down business operations entirely, impacting your ability to care for patients. That might sound dramatic, but it is an entirely plausible scenario of what can occur if an attacker is given an easy opening into and throughout your network with little to no resistance. Those of us who work in the cybersecurity defense industry all echo the same adage to our clients: Hackers can attack as often as they like; they only need to be successful once. This scenario puts on the onus on practices to always be on alert.

Unfortunately, it is not realistic to expect your practice to be able to successfully ward off every attempted attack in perpetuity. There are far too many variables, including your clinicians and staff, your third-party vendors and service providers, new technologies and systems, and ever-evolving attack tactics. Because maintaining a 100 percent prevention rate is impossible, it is crucial to have a plan in place for response, mitigation, and recovery.

> Careful preparation should be the first element of your incident response plan. Responses to cyberattacks should not be an entirely reactionary function; careful planning, preparation, and training can serve as significant risk mitigators.

Responses to cyber incidents should follow a playbook. Regardless of the size of your practice or where you are located, your cyber security procedures should be the same. The following is an outline of what a cyber incident prevention and response plan should look like, the questions you should ask of yourself and your information technology (IT) or security team, and what you should do in the event of a worst-case cyberattack scenario. In general, an ideal cybersecurity incident response plan should:

- Assemble an incident response team.
- Detect and analyze potential security threats.
- Disclose incidents when they occur.
- Contain any damage.
- Eradicate identified vulnerabilities.
- Conduct a post-incident analysis.

Prioritize Your Threats

The types of events that may trigger an incident response protocol can vary greatly, and you should take all of them seriously. Your team should not only respond to perceived catastrophic events. For example, within a hospital network or clinic, thousands of indicators of potential security incidents may appear each day. An organization typically logs these events, and they can provide an abundance of data that companies can mine for prevention purposes. These data can be filtered using automated techniques, yielding valuable information that IT staff can use to identify whether a security incident has occurred.

Incidents should be prioritized based on their functional impact and the time and resources needed to recover, not dissimilar from the triage approaches used by healthcare providers. If you are unsure which incidents you should prioritize in your organization, you may want to start by performing a business impact assessment to identify your most pressing security concerns. Classify the types of adverse situations your practice may encounter into three separate categories:

1. Events
2. Security incidents
3. Breaches.

These categories should dictate your team's response. For example, a compromised endpoint, such as a phishing email that was clicked on a laptop, should be classified as a security incident. Should the phishing malware take hold of critical systems, such as your electronic health record or billing software, that occurrence should be classified as a breach.

The term *breach* is often considered a four-letter word. As with most words, though, its true meaning is rooted in context. For example, although you might not have a *Health Insurance Portability and Accountability Act (HIPAA) breach*, you could still have a *contractual breach*. You should attempt to use uniform nomenclature in your internal documentation for the sake of clarity, particularly regarding your information security policy and incident response plan. Review the language in your contracts to ensure terms are consistent and mutually understood.

In any instance of a security compromise, taking the following steps can provide a standardized roadmap for organizations to address the cyber risks that threaten them and respond appropriately with established incident response plans.

Be Proactive

Careful preparation should be the first element of your incident response plan. Responses to cyberattacks should not be an entirely reactionary function; careful planning, preparation, and training can serve as significant risk mitigators.

In the early steps of incident response, it helps to have ready access to continually updated information about your personnel, assets, and processes, including items such as contact information for team members, network diagrams, computer inventories, templates for documenting security events, spare computers for gathering evidence and analyzing forensic information, and an incident reporting mechanism through which employees can proactively report suspected attacks.

Organizations should take proactive measures to address potential disruptions in business operations, including:

- **Performing risk assessments.** HIPAA security rules mandate that organizations undergo risk assessments annually. We recommend risk assessments that include an exhaustive vulnerability analysis of technical resources to get a full picture of your risk landscape.
- **Ensuring endpoint security.** "Endpoints," such as servers, laptops, and workstations, should be appropriately secured, incorporating permissions controls according to individual job tasks and implementing configurations in accordance with HIPAA technical controls. We recommend forgoing traditional antivirus software in favor of next-generation antivirus products that are inclusive of response functionality.
- **Enforcing network security.** Firewalls, virtual private network activity, and connections to vendor resources should be configured, produce log reports, and be reviewed regularly.
- **Conducting security awareness training.** HIPAA requires annual security awareness training, which should be expanded to include conducting simulated phishing attacks and providing employees access to additional resources to foster a security and safety-first culture.

Assemble an Incident Response Team

A cyberattack can unleash a flurry of activity. For many of us, our first instinct is to try to reset everything back to the way it was. Unfortunately, when an attack of unknown significance occurs, even the most seasoned of practice administrators, healthcare professionals, IT professionals, and others may be tempted to opt for the "pretend nothing happened and hope for the best" approach—which is the absolute worst way to react to an adverse event.

Even if backups are readily available, the best practice is not to "sweep things under the rug" and revert to a backup immediately. Why? Because reverting to a backup will remove the crucial clues and evidence of what has happened. If you destroy the traces of what the hostile entity did, you will have a much more difficult time figuring out what needs to be repaired, dealt with, and remedied to ward off future attacks. The best course of action is to remain calm and follow the incident response procedures you have established.

Assembling an incident response team should be your first action toward creating an effective response plan that you can mobilize in the case of a security incident or breach. Your team should include IT management, security personnel, the appropriate representatives of senior management, and, in the case of a breach, representatives from the affected departments. Depending on the nature of the attack, the team should also include representatives who manage affected or essential systems, such as electronic health records, medical imaging equipment, payment software, claims management, and others, as necessary.

Outsourced resources can be helpful in performing the skilled portions of incident response work, such as security assessments and forensic investigations. Off-site managed security services providers can provide ongoing monitoring of endpoint protection,

cloud applications, firewalls, and other security devices. These organizations can help temporarily or permanently augment staff to fill gaps in security-specific knowledge or specialized software. These vendors can also provide economies of scale to lend assistance when additional security resources are needed.

Detect and Analyze Potential Security Threats

After creating an incident response team, your next step to help ward off cyberattacks is to detect and analyze potential security threats. This step will help you understand what may attack your organization and the implications of any potential attack. Gaining visibility into your systems and their weaknesses in this preparation phase can help you lay a foundation for knowing where to look for potential security incidents, how to manage alerts, and how to determine the extent of any damage caused by an attack.

Security incidents can occur in a seemingly infinite number of ways, and coming up with strategies to combat each one individually is not feasible. However, cyberattacks in the healthcare industry take fairly predictable forms: phishing, unpatched vulnerabilities, insider threats, network attacks, and web application weaknesses.

Developing visibility adequate to accurately detect whether a system has been compromised takes time. Sometimes it can take years of detection to accurately understand a given network and adjust logging and alerting processes to be able to provide actionable information in the event of a cyberattack. If you believe that your program or practice is entirely free of adverse programs, such as malware, it may just take a closer look to uncover it.

Detection can be enhanced by focusing on some of the more obvious indicators of compromise, including firewalls, traffic going in and out, antivirus software, and server logs. One of the easiest ways to gain visibility into a potential issue is to ask your clinicians and staff to report suspicious network behaviors, through either a support system, email inbox, or informal questions. It is important for incident responders to address both big and small issues with care, because simple network pings traveling outside the United States can lead to discovery of entirely compromised systems.

Analyzing suspicious indicators once they are detected can be a daunting task, and it often comes down to experience and judgment. Due to an abundance of false positives, system malfunctions due to configuration issues, and human errors, detection can become a full-time job. Some incidents—such as ransomware or a defaced website—are easier to detect than others, but often the ones we should be looking for are hidden in logged data. Whether you are actively responding to a security incident or creating the foundation for an evidentiary logging structure, it is important to rely on security professionals to set processes up correctly.

When a security incident occurs, your documentation of the event should detail:

- The source or initial suspicious behavior noticed.
- The summary of the incident as it continues to transpire.
- Log data.
- Specific dates and times.
- Actions taken by staff.
- Steps intended to remedy the issue.

When properly documented, detection and analysis become the catalysts for information sharing, incident prioritization, and understanding the technical impact and material risk to the organization. We recommend retaining a firm that specializes in breach response and then establishing a retainer with the vendor. Often, a baseline relationship can be established without cost to avoid slowdowns in analysis, which may be hindered by legal negotiation and contracts.

Disclose Incidents When They Occur

During the course of detecting and responding to a security incident or breach, the question of how and when to communicate the event to others—partners, vendors, clinicians and staff, law enforcement, patients, regulatory organizations, insurers, and more—will arise. The appropriateness and nature of these disclosures should be considered carefully and ethically and evaluated with your legal counsel. Your counsel can also provide information about the necessity of disclosing the event to your patients based on Health and Human Services and Office for Civil Rights requirements.

Contacting law enforcement officials is typically a necessary step, although engaging with them incorrectly, or too early, may reduce their efficacy. For a variety of reasons—including a lack of law enforcement personnel resources, poor investigative capacity, and the abundance of attacks outside the United States—the apprehension and conviction of cyber criminals is not what we would hope or expect. Law enforcement may be able to give you some guidelines on how to provide digital forensic information to them after you have activated your response plan. It is important to engage with law enforcement after an attack, especially if you are seeking a legal remedy or making a cyber insurance claim.

Contain Any Damage

Containment strategies—including quarantining machines, locking down a network, or simply turning machines off—should be determined based on the type of cyberattack you sustain. Containment operations may even be automated to some extent if you are leveraging advanced products to protect your endpoints. Most incidents require some level of containment, and this measure can be critical in preventing damage spreading to additional systems. Containment strategies should include considerations for potentially lost or stolen devices, evidence gathering and preservation, how much of a system to contain, and estimated time to recovery.

In previous security incidents, we have had to temporarily shut down entire elements of a medical practice to give ourselves time to determine how we should proceed in the aftermath of an attack. This pause took down medical device functionality for a short period of time, but it allowed us to make network configuration changes, gather evidence, and address concerns from a compromised vendor with little impact on patient care.

Eradicate Potential Vulnerabilities

Too often, eradication and recovery are prioritized during the security incident response process. These steps should only begin after the preceding steps—detection, analysis, disclosure, containment—have taken place. Though continuing patient care and avoiding disruptions to a practice are truly high priorities, mishandling an incident response process and not learning from it can have a severe impact on your entire healthcare organization down the road should another compromise occur. It is essential to first understand the nature of a given attack and its full impact to determine what the next appropriate steps should be. Moving forward too quickly with a backup could cause you to miss persistent mechanisms that may have been put into place by the entity seeking to harm your practice, potentially re-infecting the devices restored by your backups.

For many medical practices, it can take months to identify and mitigate all of the vulnerabilities exploited in a cyberattack, return systems to normal operation, and confirm that affected systems are now functioning correctly. When responding to an incident, we often leverage forensic and incident response tooling to protect systems while they are being patched, removed of malware, and otherwise secured to a greater degree. This process is not always simple, and we have clients that are still challenged with defining a "new normal" even a year after a breach has been contained.

Conduct a Post-incident Analysis

You may be tempted to break out the champagne after the "successful" resolution of a security incident. We tend to rationalize our mistakes and then simply move on. But identifying lessons learned after a cyberattack is a critical piece of the incident response process, although something that is often skipped. If you do not measure, reflect, and grow from a cyberattack, you are likely doomed to repeat any mistakes again. Conducting a post-mortem to uncover what you could have done better is essential. Doing so will help you better understand the full scope of what happened, how your staff performed, what information you could have benefited from sooner, and any actions taken that may have inhibited the successful recovery of your organization.

This is also the time to deploy your evidence gathering and retention plan. Often we do not fully understand the scope of an incident that has occurred, so housing evidence to give to an external security team, industry regulator, or legal team is a helpful step in ensuring that you are not destroying evidence that may be helpful in the future.

There are many reasons why cybersecurity concerns are not prioritized in medical practices and other organizations. Whether due to the daily demands of treating patients and keeping a practice running smoothly or uncertainty over what you should do to protect yourself from cyberattacks or respond to one should it occur, the worst thing for your practice is to do nothing.

By anticipating and preparing for a potential cyberattack, you can proactively mitigate any damage that hostile actors may be able to do to your network, your data, and your patients' personal information. Creating a thorough incident response plan will give you the peace of mind that comes with knowing that you and your team will know what to do if something happens.

Sean Hall is the CEO and Adam Rebhuhn is the COO of Firm Guardian, Inc., with offices in Austin, Tex., and Madison, Wisc.

Eight Simple Steps to Create a More Secure Practice

1. **Practice good cyber hygiene.** It is important to address the IT basics, such as backups, automated updates, limited user privileges, and multifactor authentication.
2. **Segment your networks.** This makes it hard for hackers to move around and infect multiple systems. It may be a challenge for healthcare providers with multiple small clinics, but it can be accomplished when properly prioritized.
3. **Look into automating processes and outsourcing elements of your security and IT.** The scope of information technology is so vast that specialized and well-trained employees are often a necessity.
4. **Increase the amount and retention of critical logs.** Evaluate which of your areas are logging properly and where improvements can be made. Nothing makes a response process more difficult than having little to no information to start the investigation.
5. **Plan incident coordination with external parties in advance.** Organize relationships with security professionals, cybersecurity lawyers, cyber insurance companies, and law enforcement entities.
6. **Evaluate changing your antivirus software.** If you are still using a traditional antivirus, there are much better options that are significantly more effective and provide incident response capabilities.
7. **Perform a risk assessment.** Risk assessments should include an exhaustive evaluation of your vulnerabilities that address your quantifiable risk with a focus on adherence to HIPAA controls.
8. **Review or create an incident response plan, disaster recovery, and business continuity policy.** Let the frameworks and processes you develop take the lead in creating a standard that supports your healthcare organization.