All It Takes Is One

BY ALTI RAHMAN, MHA, MBA, CSSBB

Securing your practice against cybercriminals

All it takes is one. One person, one email, one click, to grant cybercriminals access to your confidential files, your applications, and your patients' protected health information. But the damage that can result from a cybercrime can often be prevented by adequately safeguarding the information entrusted to your practice. The adage, "an ounce of prevention is worth a pound of cure," holds true.

It is important to understand why healthcare breaches are so valuable to cybercriminals. The healthcare industry is entrusted with some of the most sensitive information about individuals, and adequately protecting that information requires enforcing physical, clinical, and digital safeguards. Upholding patient trust is essential to the foundation of the provider and patient relationship. The information provided by a patient should be held in confidence and safeguarded by that patient's entire care team. Given that patient information is typically stored in any one of a variety of electronic documents, applications, and systems, protecting that information is not always straightforward.

Cybercriminals understand how vital the preservation of patient trust is to healthcare systems, and they seek to exploit that. Each year, the cost to healthcare systems resulting from cybercriminal activity totals in the billions, approximately $408 per compromised patient chart. Breaches affect both public and private organizations, with between 5,000 and 25 million patient charts affected in each incident.[1] Cybercriminals are equal opportunity offenders; the nature or size of your practice is immaterial to them.

Responding to cybercrime has less to do with employing countermeasures should your data become compromised and more to do with instituting a culture that makes those countermeasures unnecessary.

A Different Type of Crime

On June 19, 2017, Oncology Consultants, a physician-owned oncology practice with multiple clinic locations across the city of Houston, suffered a ransomware attack that disabled the servers that hosted our email system, information systems (including billing), and shared drives. Without access to email, we immediately lost one of our primary methods of communication. We were suddenly unable to process claims or access practice management systems, spreadsheets, or documents.

As the practice administrator, I recall receiving a text that day at approximately 7:00 am from one of our managers, who indicated that our email and billing systems would not open. I assumed that it was a minor network connectivity issue that perhaps

Cybersecurity is not about how many thousands of dollars you spend to create a digitally secure working environment; it is about how you incorporate good digital hygiene into your daily operations.

required a server re-start. But when I arrived at the practice, I was presented with the hacker's message, demanding money in the form of bitcoin in return for the decryption keys necessary to retrieve our encrypted data.

When faced with a significant criminal act, the first reaction of many people is to call 911 and await the arrival of police officers to inspect for ongoing danger and damage and collect any evidence of the crime. Video monitoring systems, fingerprints, license plates, eyewitnesses, and other evidence can provide clues with which to identify the perpetrator and lead to their apprehension.

Unfortunately, cybercrime is unique, and none of these remedies are likely to track down the culprit. Unlike a crime that leaves physical evidence, the nature and extent of a cybercrime may not be immediately apparent. When you cannot access a desired document or program, your first attempt at a remedy is often to power your computer off and on again. If the problem does not go away, you may escalate it to your local information technology (IT) resources. Unlike in the aftermath of a physical crime, there is yet no indication that any crime has been committed. You have not yet made a connection between your lack of access to your files and a criminal action that may have significant consequences to your practice. In the meantime, the cybercriminal is left to roam freely through your encrypted databases, picking and choosing what information they want to steal from your digital space.

A Culture of Security

Responding to cybercrime has less to do with employing countermeasures should your data become compromised and more to do with instituting a culture that makes those countermeasures unnecessary.

Your organizational culture encompasses both the mundane and the essential. What you wear to work, the hours you keep, the level of professionalism among staff, and organizational hierarchy all reflect the unique culture of a workplace. So, too, do your practice's mission, values, and vision. All of these variables affect not only the morale and professional satisfaction of your staff but also how your patients feel about your practice and their treatment there.

Culture does not have a distinct moment of conception or of termination. Rather, it evolves organically and can change over time. The attitudes and behaviors of a practice's management staff are often reflected—for good or for bad—in the demeanor of front-line practitioners, administrators, and staff. Organizational culture is the common denominator of all of your operations. As such, culture is incorporated into your organization's approach to maintaining and promoting a safe digital environment for your practice and your patients.

Your practice's culture should promote the understanding among staff that cybersecurity is everyone's responsibility. Each employee should have a baseline understanding of what cybersecurity is and why it is essential. Everyone should know how to maintain a secure digital environment and how to detect potential hacking attempts. This effort requires a continual conversation between management and staff so that everyone fully understands their role in preventing and heading off potential attacks. Cybersecurity is not about how many thousands of dollars you spend to create a digitally secure working environment; it is about how you incorporate good digital hygiene into your daily operations.

Four simple policies are foundational to creating an effective cybersecurity awareness culture in any practice.

Policy 1. Beware the Suspicious Email

Email is the lifeblood of communication in the modern-day workplace, and cybercriminals have become sophisticated in using emails to dupe employees into unwittingly granting them access to sensitive information. In their efforts to trick employees into clicking links that enable unauthorized access to information, cybercriminals will disguise the origin of emails and use language that indicates that immediate action is required to resolve a claim, ensure a shipment, or pay an invoice.

More sophisticated cybercriminals will impersonate the identities of upper management to convince staff that an email is an urgent request from a supervisor. Such messages can evoke an emotional response from the receiver, who may unthinkingly do what they are told, enabling a potentially disastrous security breach.

But proactively heading off such attempts can be effectively accomplished by teaching staff how to quickly spot dubious emails and determine the sender's true identity. Staff can be easily taught to determine whether a given email is questionable and how to check the identity of the source of a message. If staff are even remotely suspicious of the true intent of an email, they should be directed to put safety first and delete the message or report it to the appropriate IT resource for review.

Policy 2. Resist Surfing

Cybercriminals well understand the siren song of the internet. Having the world at your fingertips has brought much good into the world. But it has also heralded an insidious—and lucrative—form of crime. There are many available tools that can block web browsing and help your staff steer clear of malicious websites. But these tools cannot always keep pace with the rate at which new malicious sites are launched or new ways of bypassing security measures are created. Ultimately, unless you completely disable internet access across your organization, you cannot be completely protected.

The best prevention remains having your staff limit their use of the internet to workplace needs only. Doing so can significantly reduce the surface area on which a cybercriminal can gain footing.

Policy 3. Practice Password Hygiene

The healthcare industry, more so than others, is required to use different systems for multiple reporting, invoicing, and storage purposes. There is no magical application that does everything. With multiple systems comes the challenge of creating and remembering multiple passwords to gain access. For many, the natural tendency is to use the same password for multiple systems or to create a simple password such as "12345" or "password." Cybercriminals look to exploit these shortcuts. They know that in many cases, obtaining one password will grant access to additional applications that use the same password.

It is essential to require all staff to create alphanumeric passwords that incorporate at least seven characters and change their passwords regularly. Modern-day applications are configured with minimum password requirements and the ability to prompt users to change their passwords at a specific frequency. Another popular method of maintaining password security is to employ two-factor authentication, in which users must authenticate their access to an application with both a password and a secondary method, such as a text, telephone call, authentication service, or a physical security USB key inserted into a computer.

Policy 4. Log Off and Turn Off

When a cybercriminal attempts to access your digital environment, there may be indicators that an attack is in process, such as slowed performance or unexpected malfunctions. But just as burglars know that their chance of a successful robbery is improved when you are not in your home, cybercriminals understand that after-hours break-ins are less likely to be detected.

When your staff leave the office at the end of a day or over a weekend, workstations are unattended and fewer eyes are guarding your data. This is the ideal time for an attacker to attempt to access your systems. The most straightforward way to protect your assets when your office is empty is to require employees to log off any applications and shut down their computers when they are away.

Organizational Safeguards

In addition to creating an organizational culture that emphasizes the responsibility of individuals to maintain digital security, there are foundational components to securing your digital assets. No matter how proactive you are in teaching your staff to safeguard their computer access, all it takes is one person to make an honest mistake and the door to cybercriminals is open.

Each of the four safeguards detailed below incorporate people, processes, and technologies that together can build organizational protection against cybercrime.

Safeguard 1. Develop Vendor Security Assessments

The healthcare industry, like any business, relies on multiple information systems to maintain operational areas, including compliance, clinical, finance, and accounting. These systems must be able to communicate with one another to exchange and update relevant information. Both protected health information and personally identifiable information may be stored and exchanged among your systems, increasing opportunities for cybercriminals to gain access to sensitive data.

> To continually maintain robust cybersecurity measures, healthcare organizations should assemble a multidisciplinary, interdepartmental information security committee.

A vendor security assessment is a document with a mix of checklist-style and narrative-based questions designed to assess the security elements of the applications you currently have or desire to have in the future. These assessments are designed by security and legal professionals to help you understand both the technical and legal risks associated with working with a digital vendor and/or service provider. Before working with a potential vendor, you can use vendor security assessments as part of your due diligence process of vetting your vendor's security protocols. This can help you more fully understand the vendor's cybersecurity protections and response procedures. In the event of a cybersecurity breach, these assessments can determine the respective liability of each party involved. Vendor security assessments should be updated at a specific frequency (i.e., annually) or when the nature of a business relationship or services change.

Safeguard 2. Create an Information Security Committee

To continually maintain robust cybersecurity measures, healthcare organizations should assemble a multidisciplinary, interdepartmental information security committee. These committees meet regularly to ensure that an organization's information security objectives concerning networks, software, hardware, and data flow are being met. The extensive nature of organizational cybersecurity requires information security committees to define their scope in terms of team members, meeting frequency, purpose, tasks, budget, and goals.

Committee members should represent the various levels of functions in a given organization, including direct decision makers, managers, subject matter experts, and daily users. It is advisable to maintain a set of core members who meet regularly and an ad hoc group that attends depending on the issues being discussed or the projects being reviewed.

An essential function of an information security committee is to translate operational objectives into training and, ultimately, the culture of how users interact with information systems. Committee members should translate the technical jargon associated with information security into identifiable goals by communicating practical examples of how to engage with systems and the consequences of inadequate cybersecurity hygiene.

Because failure is often inevitable in this realm, it should be treated as a valuable lesson. The information security committee should develop post-failure mitigation strategies to limit the scope of the potential damage that can be done to an organization in the case of a cybersecurity breach.

Safeguard 3. Encrypt Sensitive Data

Protected health information and personally identifiable information are coveted items for cybercriminals. Often, these data reside in multiple places, because many staff members may need access to perform their jobs. Analysts may need to store information on their local workstations or laptops to turn patient data into information. Many of the tools of data analysis, such as Excel spreadsheets, require data to be stored on local drives, creating a risk in the event that a laptop is compromised via theft or unauthorized access.

One effective measure to prevent sensitive data from being compromised is to protect workstation hard drives with encryption technology, which makes it much more difficult to access data. Due to the technical nature of encryption, it is essential to consult with IT security professionals to learn about the various types of encryption technology available and the pros and cons of each.

Safeguard 4. Obtain Cyber Liability Insurance

Cyber liability insurance provides a safety net against the extensive costs that may be incurred in the event of a cybersecurity breach. Depending on the structure of the coverage purchased, covered costs may include expenses incurred for hardware replacement, regulatory defense, network assets, cyber extortion, and disciplinary fines. As is the case with all insurance, it is best to be proactive and obtain this insurance as a preventive measure rather than purchase it after a breach has occurred.

Adopting good cybersecurity practices lies at the intersection of user policies and organizational initiatives. Just as the practice of medicine hones clinical skills, provides experience, and ultimately improves patient outcomes, continually practicing good cybersecurity protects the digital health of your organization.

A proactive cybersecurity strategy is most effective when there is collective buy-in from the top of the organizational structure to the front lines. Assigning a budget to cybersecurity protocols is secondary to developing and implementing the rules that guide our work in the digital sphere. Consistently adhering to those rules is crucial, because cybercriminals are relentless, knowing that all it takes is one person, one email, or one click to gain access to your most sensitive information.

A Look Ahead

A few months after the ransomware incident at Oncology Consultants, the attackers ceased communications with our practice. At the onset of the incident, we used a forensics firm to review our network, server, and workstation environment to ensure that the invisible criminals had been removed. Upon completing a forensics report, we reported the incident to the Office of Inspector General and then completed a network security audit and improvement process with the aid of a cybersecurity firm. We retained that firm to provide 24/7 monitoring of our network. We now run annual exercises and hold educational sessions within our organization to maintain continual vigilance of potential cyberattacks.

In 2020, the advent of COVID-19 has led to a rapid expansion of telemedicine, creating more opportunities for cybercriminals to exploit. Though companies can exercise control over their own cybersecurity, patients may not have similar protections in place. More work is required to create security barriers, especially as healthcare moves to a hybrid model of digital and face-to-face interactions.

In the long term, healthcare will continue to move from a referral-based transaction to a consumer-driven one that more resembles industries such as retail, automotive, and air travel. Such convenience will require heavy investment to keep secure a proliferation of technologies in the form of apps, digital wearables, and mobile diagnostic tools. As consumer-driven healthcare becomes more commonplace, we must stay vigilant to growing cybersecurity threats looking to exploit any doors left open in our digital homes.

Alti Rahman, MHA, MBA, CSSBB, is practice administrator, Oncology Consultants, an oncology practice with multiple clinic locations across the city of Houston.

Reference

1.Morse S. Healthcare's number one financial issue is cybersecurity. Available online at: healthcarefinancenews.com/node/139027. Last accessed July 22, 2020.