Smart Business Great Medicine

Whitepaper

Cybersecurity Guide

By Paul Cox

Cybersecurity Guide for Medical Practices

Although nothing will guarantee 100% protection against cybersecurity threats, there are steps all medical practices can take to significantly reduce the risk of becoming victim to hackers. It is imperative to implement a **Cybersecurity Checklist** and review it on a regular basis because of the ever-changing nature of cybersecurity threats.

Cybersecurity Risk Assessment

A cybersecurity risk assessment is a crucial part of risk management for every medical practice. All aspects of a practice rely on information technology and systems to conduct everyday business and care for patients—from phone systems to electronic health records. Beginning with a risk assessment will help you prioritize other items in this guide.

Risk assessment is used to identify possible risks, estimate likelihood of occurrence and levels of potential loss from risks, and prioritize actions that can reduce risks or assist in recovery if those risks occur. It is important to consider all risks to operations ((eg, mission, functions, image, and reputation), assets (eg, personal information, health-related data, business records), individuals (eg, partners, staff, patients), other organizations (eg, hospitals, clinicals, insurers), resulting from the operation and use of your information systems.

Most formal risk assessments follow the National Institute of Standards (NISTs) guidelines. Formal risk assessments are typically conducted by third-party companies specializing in quality improvement, risk assessment, and/or cybersecurity. Undertaking a formal and thorough risk assessment may be time consuming for medical practice staff. Whether from outside professionals or inside staff, it may not be practical for small or midsize medical practices to do formal and quantitative risk assessments. In these casees, a qualitative risk assessment may be more practical and can still provide real value for a practice to reduce cybersecurity risks.

Qualitative Risk Assessment

A qualitative approach addresses how the practice will be affected by a potential risk and how the services we offer and people we serve be affected by a loss?" This view is much more subjective than its quantitative counterpart in that it seeks the opinions

and viewpoints rather than specific numbers and percentages of a formal risk assessment.

A qualitative assessment requires three components:

1. A list of the key components to the practice. These components may not be the most valuable but instead are the most essential to keeping the practice operating, including employees, access codes, passwords, computers, phone systems, electronic health records (EHRs), customer information, network, documents, fax lines, facilities, and more. Start as comprehensively as possible and then prioritize assets by whether none, some, or all the practice services could continue without that asset.

2. A list of vulnerabilities associated with the assets that, if compromised, would limit or stop practice operations, especially in users and IT components. For example, users are susceptible to social engineering, and a vulnerability scan on IT components will undoubtedly turn up missing patches and insecure configuration.

3. Develop a list of possible threats (eg, social engineering, loss/theft, hacking) Although many may not be known specifically because hackers can be anywhere in the world and are always evolving new methods, the latest, most common threats are listed and described at network security companies, such as Cisco or Juniper Networks.[2,3]

Addressing these risk assessment components will lay the groundwork for developing a business continuity plan (BCP) to prevent and detect risks and minimize damage and promote recovery if cyberthreats occur.

Cybersecurity Checklist and Plan

Small practices are as vulnerable to cyberattacks as large hospitals. Although there is no 100% guarantee against cybersecurity threats, taking the right actions can significantly reduce the risk of your practice becoming a victim of hackers. Having an action plan and checklist are extremely important to ensure everyone in your office has the training to fully understand what their responsibilities are for safeguarding the computer network and both employee and patient data. See our sample **Cybersecurity Checklist**. Download a copy of this checklist to post in your office by activating a free membership on our website:

www.SmartBusinessGreatMedicine.com.

Cybersecurity Checklist

To protect your practice from cyberattacks:

- ☐ Implement a secure password policy
- ☐ Address insider threats (both intentional and unintentional)
- ☐ Encrypt data
- ☐ Manage virus protection software
- ☐ Update software regularly
- ☐ Train employees in an ongoing manner
- ☐ Make cybersecurity everyone's responsibility
- ☐ Have data back up and disaster recovery plans
- ☐ Perform yearly cybersecurity risk assessment

Visit www.SmartBusinessGreatMedicine.com to learn more about cybersecurity and Using Health Care Information Technology!

A Secure Password Policy

Strong passwords are the first line of defense for protecting the computers and network in your practice. According to Verizon's annual Data Breach Investigations Report,[4] 81% of hacking-related data breaches involved stolen or weak passwords. Physicians and practice managers should take note of this important statistic and not only ensure they use a password policy but also institute training to ensure everyone understands and follows the policy.

Here are some best practices, which are also covered in our downloadable infographic also available to members of Smart Business Great Medicine.

- Make passwords at least 8 characters long; longer is better. Longer passwords are harder for hackers to crack. Consider using passphrases such as "I went to Emma Samson High School in 2001" and use the initial of each word as in "Iw2ESHS#2001." Include a number, upper case letters, and symbols (eg, #, ! , or $)
- Do not use a word that can be found in a dictionary—hackers have programs to exploit this type of password
- Do not use birthdates, anniversaries, or people's or pet's names, which can also be easily exploited
- Change passwords every 60 to 90 days

- Do not leave a password in plain sight. This may seem obvious; however, many people write their password on a yellow sticky note and leave it on their computer or in a top drawer
- Consider using a password manager application. Programs or web services let you create strong passwords for each account. These programs can also be used to remind and/or require employees to change their password regularly
- Consider multifactor authentications. Set up multifactor authentication that requires a code be sent to an individual's phone. This way hackers cannot access without having physical access to that phone

For an in-depth review, see the National Institute of Standards' Guidelines for Digital Identity Authentication and Lifecycle Management.[5]

Insider Threats

You can't run a medical practice without giving employees access to resources, and you can't give them that access without some degree of risk. This is especially true for small to midsize practices in which individual staff members often fulfill multiple roles and have significant access patient records, physician information, and company financials.

Insiders can damage your practice in countless ways, from destroying valuable equipment or stealing money, to leaking sensitive data or providing access to unauthorized third parties. These incidents can lead to lost revenue, compliance fines and lawsuits, and serious damage to your reputation.

An insider-threat program can help you anticipate and address risky or destructive individual behavior before major damage is done. However, it is crucial to address insider threats based on a realistic assessment of risks. Most practices face far more danger from lack of attention or training by insiders than from actual malice. Fostering a collaborative culture of security will earn employee buy-in and provide better results (and morale) than a top-down "everyone is a suspect" approach. Insider threats can be categorized into four groups:

Privileged users

Administrators and database operators who have direct and unrestricted access to sensitive information are privileged with that informaion. These individuals comprise what is probably the most dangerous group, because they are the most trusted insiders. Data theft and fraud for personal gain are unfortunately not rare, and mistakes by system administrators can have severe consequences.

Remote subcontractors

Remote employees and third-party partners have access to your sensitive data. The catch is that although you may be confident in your own security, you do not actually know that much, or anything, about your partners' security policies. It is important to monitor the actions of remote subcontractors and make sure they are not misusing your data.

Former employees

Disgruntled employees can sometimes try to take revenge on a company after leaving. Sometimes, recently terminated employees may try to steal your data and use it to start a competing business or take it to your competitors.

Inadvertent insiders

Not all insider attacks are deliberate. Sometimes employees leak sensitive data online completely inadvertently, for example by sending an email to the wrong recipient. Such mistakes can go undetected for a long time, causing damage that translates into severe remediation costs when the incident eventually comes to light.

Internal Controls and Responsibilities

No matter the reason for insider vulnerabilities, whether malicious crimes, negligence, or lack of training, all insider threats or attacks are both difficult to detect and very costly to remediate. This is because employees have legitimate access to sensitive data, making it extremely difficult to distinguish between misuse and actual work routines. It is impossible for a practice manager or physicians to realistically be able to monitor every single aspect of a practice. This does not mean nothing can be done, and there are key actions to mitigate insider threats.

Assign owners for each component of the practice (eg, Human Resources, Physical Security, Data Owners, Finance, and Information Technology (including your EHR). Have the security owner for each area regularly monitor/assess components for which they are responsible and have them provide reports of these assessments to the practice manager and partners. Consider putting quarterly or biannual reminders to complete these assessments into the practice calendar. Ensure all employees know how and to whom they should report any security concerns in any one of these areas.

Cultivate a Culture of Security Awareness

The most important measure any business, including medical practices small and large, can take is to train all employees regarding how insider threats can damage, or even destroy,[4] a company, its reputation, and its staff. Instill the understanding that it is everyone's job—not just IT's—to help guard against these schemes. Teach employees cybersecurity best practices and how to perform their jobs to limit risk encourage them to be vigilant for warning signs that the company has been or could be victimized—from observing suspicious behavior to identifying a weakness in the system that could be exploited. Provide employees with specific information about how to respond if they have any cybersecurity concerns.

Additional guards against insider threats include:

- Develop and enforce a process for when an employee leaves the practice for any reason
- Hire only credible 3rd party contractors who are licensed and have high recommendations
- Leverage the risk assessment to determine critical assets
- Create a written insider threat policy for each component of the practice
- Leverage auditing and monitoring technology
- Use due diligence and background checks during the hiring process
- Pay attention to your employees' well being

Virus Protection Software

Antivirus software is the first line of defense against cyberattacks. For single-physician practices with a couple of computers, a do-it-yourself approach of installing off-the-shelf antivirus software may be adequate. In this scenario, it is critical to turn on automated updates or at least manually update the software regularly, although the latter is less ideal because it requires each individual make updates on their computer.

Ideally, a practice will have a managed network security solution encompassing antivirus, antimalware, firewalls, email security, and intrusion prevention systems (IPS). Such solutions lift the burden off individual staff

members and centralize control of antivirus software to a dashboard application that manages all computers in the office. Centrally managed software protects the practice network and all connected computers from a variety of threats. Centrally managed software also updates programs automatically, so individual staff members do not need to update or scan their machines on their own, and everyone in the practice has the most up-to-date versions at all times.

The next level of network security is endpoint security or endpoint protection, which encompasses provisions for determining which applications (programs) can be installed (ie, whitelisting), setting network access controls (ie, permissions and passwords), detecting unusual activity (ie, endpoint detection/response), and monitoring tools and logs to safeguard the various endpoints of the network. Examples of integrated network security solutions include Bitdefender, F-Secure Protection, Symantec, Avast, Kaspersky, and Trend Micro.

Software Updates

Maintaining software updates is another foundational cybersecurity practice. Start with setting operating systems (eg, Microsoft Windows or MacOS) for automatic updates. For instructions to install operating system updates, visit the Microsoft[6] or Apple[7] websites. It is equally important to update Microsoft Office applications,[8] especially Outlook, because many hackers will hide malicious software in files that appear to be Microsoft documents. Updates can be automated, which is recommended, or manual. System updates are just as important for server operating systems (your network operating system) for which all patches and updates need be reviewed and updated on a recurring and regular schedule.

It is also important to update your web browsers because most physician offices utilize web-based applications (eg, portals to verify patient insurance). Use the most current version of the web browser software available (eg, Internet Explorer, Chrome, Safari, or Firefox) and enable automatic updates, if possible.

Employee Training

Most medical practice staff members of a are already overworked with scheduling patients, verifying insurance, obtaining prior authorizations, completing paperwork, and a million other things. Despite these hectic schedules, it is up to the leaders and managers of the practice to ensure everyone is trained and fully understands the cybersecurity policy and best practices. Survival of the practice may depend on it. Training should include education about the importance of cybersecurity, setting up and managing passwords, being aware of suspicious emails (and what a suspicious email looks like) and what to do if there is an incident. Training should not be a once a year activity–it should be done on a regular basis to make staff aware of the latest best practices and threats, or simply reinforce previous training.

Data Backup and Disaster Recovery

There's an old saying that business owners who are responsible for data backup fall into two categories: those who have lost data and those who will.

Medical practices generate large amounts of data and data files are changing throughout the workday–much of it containing protected health information (PHI). Data can be lost, corrupted, compromised, or stolen through hardware failure, human error, hacking, or malware. Loss or corruption of data could result in significant business disruption.

Make data backup and recovery an integral part of your BCP and IT disaster recovery plan. Begin by identifying what data to backup, selecting and implementing hardware and software backup procedures, scheduling and conducting backups, and periodically validating that data has been accurately backed up.

When a medical practice is disrupted, it can cost money. Lost revenues plus extra expenses means reduced profits. Insurance does not cover all costs and cannot make up for patients that have not received the care they needed. Although the actions described in this guide can help prevent disasters, there are no guarantees. A BCP to continue business in case of a cybersecurity breach or other disastrous event is essential.

A BCP defines a process for prevention and recovery from potential threats to a medical practice. The plan ensures that all the staff and assets are protected and able to recover functional abilities quickly in the event of a disaster. The BCP is generally conceived in advance and involves input from key physicians and staff.

A BCP involves defining any and all risks that can affect the company's operations, making it an important part of risk management strategy. Risks may include natural disasters—fire, flood, or weather-related events—and cyberattacks. In addition to identifying

Data Backup and Recovery Checklist

To protect your practice from cyberattack backup your data regularly and have a recovery plan in place:

- ☐ Make data backup and recovery part of a larger business continuity plan
  - ☐ Backup and archive critical data daily
  - ☐ Test and verify backup process regularly
  - ☐ Encrypt backup media and store offsite
  - ☐ Update software regularly
- ☐ Identify critical files and ensure these are documented and listed in backup
- ☐ Create an emergency/incident management communications plan
  - ☐ Include who initiates and receives com munication for which incidents
  - ☐ Ensure actual contact info (not just names) are on the document
  - ☐ Identify and prepare a spokesperson to speak to press and/or public
  - ☐ Include communication with employees and their families
  - ☐ Include notifying authorities in case of a disaster or incident
- ☐ Ensure staff members understand plan and can play their role in it
- ☐ Entrust system restore procedures at least one individual outside the practice
- ☐ Review and update plan whenever staff or staff capabilities change

Visit www.SmartBusinessGreatMedicine.com to learn more about cybersecurity and Using Health Care Information Technology!

risks, the BCP identifies how each risk could affect business operations if it occurred. Safeguards and procedures to mitigate or lessen these effects can then we developed and tested. Conduct a review and test of the BCP and processes within it at least annually.

Conclusion

In today's information- and media-rich society, access to information gives us many advantages but is not without risk. Although creating a BCP, reviewing your cybersecurity practices regularly, educating all team members, and using known best practices will not guarantee safety and security, these steps will minimize risk and make any needed recovery much easier. We hope that this guide will help you take the needed steps to protect your practice.

One of our goals at SBGM is to help physicians stay secure. Follow us on social media at Twitter, Facebook, or LinkedIn or Contact Us for help with your cybersecurity questions.

References

1. https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering/collaboration-space/browse/risk-assessment-tools) .
2. https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html
3. https://enterprise.verizon.com/resources/reports/dbir/
4. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
5. https://support.microsoft.com/en-us/help/12373/windows-update-faq
6. https://www.apple.com/macos/how-to-upgrade
7. https://support.office.com/en-us/article/install-office-updates-2ab296f3-7f03-43a2-8e50-46de917611c5?ui=en-US&rs=en-US&ad=US

Smart Business Great Medicine