A PUBLICATION PROVIDED BY
MGMA MARYLAND

MediNews

JULY/AUGUST 2018

RISK AND COMPLIANCE MANAGEMENT

INSIDE THIS ISSUE

Ben Schmerler
DP Solutions

5 Ways To Protect Your Practice From Fundamental Network Security and Compliance Risks

AS SOMEONE WHO has worked in the Managed Network Services space for over a decade, there are certain behaviors I notice when it comes to security planning. Every so often, a major security incident occurs that makes headlines, and the media cycle begins. Decision makers at organizations, who are typically business experts and not technology experts, often react with questions about what they are doing to fight this specific threat. Are they doing the right thing? What else could they be doing? How exposed are they?

This kind of reactionary impulse does not necessarily bear out when it comes to other areas where we manage risk. Consider investing. Most people who are investing for the long term develop a strategy and stick to it; they do not allow some kind of external factor to force them to change their fundamental strategy, even if they make minor adjustments along the way with the advice of an expert.

While not completely the same as investing, you want to create a good fundamental approach to managing the risks associated with your practice's security. By developing strong habits, you will be managing security and compliance risks by "tweaking" your approach, rather than tearing your whole approach down and rebuilding from scratch.

Let's go over a few fundamental ways to approach security and compliance that any decision maker who has been tasked with managing this process should consider:

1.ESTABLISH AN ACCEPTABLE USE POLICY

During assessments, I often find that organizations, especially those with a dozen or so employees, lack basic rules on Acceptable Use. It is almost as if they expect users to know what the rules are and what responsible behavior means when using company owned devices and data without formally explaining it to them. It is important that your Acceptable Use policy be extensive, direct, clear, and communicated to staff, so that there is no room for misinterpretation. While we want users to have flexibility with how they use the tools available to them, they need to be aware of what pitfalls to avoid. Simply defining Acceptable Use rules leads to better outcomes and users begin to feel they have a responsibility in protecting the organization's technology assets. Having users bought into company policy about usage reduces security risks dramatically.

2.HAVE A STRUCTURED APPROACH TO MAINTENANCE

If you have technology assets of any volume, then a comprehensive plan to proactively support and maintain the system is necessary. Even in 2018, there are still organizations with significant amounts of sensitive data including ePHI, major investments in servers, and sophisticated network equipment that approach management and support reactively, or not at all. It's almost as if support is a cost they wish to avoid. However, practices that are not performing any kind of proactive management will often have high severity vulnerabilities from my experience running numerous tests over the course of my career. A security incident due to this lack of management

costs them much more money and stress than an actively managed system, which has far fewer risks of a major incident occurring. Many practices that experience downtime, data breaches and operational failures from ransomware often could have avoided the incident if the vulnerability had been patched out through proactive managed support.

3.PROVIDE REGULAR SECURITY AWARENESS TRAINING TO STAFF

While having an Acceptable Use Policy is essential, it is also a good exercise to provide some kind of basic education to end users about Security Awareness. The goal here isn't to create a team of network security experts on your staff, but rather give staff some information to identify what incidents they could experience, how to report to management, current trends and how it applies to the organization, how these concerns tie into HIPAA compliance and your patients' privacy, and so on. We want people to avoid incidents, but also minimize the damage from potential incidents by recognizing them and responding accordingly.

4.PERFORM REGULAR VULNERABILITY/RISK ASSESSMENTS

Even well maintained systems will have flaws. There are so many potential vulnerabilities, both on the PC/Server level, as well as from the outside, that it is virtually impossible to patch them all proactively. New vulnerabilities are discovered regularly, and even diligent maintenance could lead to an important patch being missed due to a variety of reasons. Regular vulnerability/risk assessments should be in place so that security issues can be fixed and adjustments can be made. HIPAA/HITECH requires risk assessments to be performed regularly as well.

5.MAKE SECURITY/RISK MANAGEMENT A PART OF THE DISCUSSION DURING TRANSITIONS

In the rush to execute a new change, like replacing an end-of-life server or implementing a new application, some organizations fail to make security a part of the discussion. I recommend focusing on the workflow first. What is it about this particular change to technology that enhances or supports the current workflow? Once that is identified, the next step is to not necessarily change the way people will work, but put security tools and policies around that workflow to improve risk management. In order to achieve that, we need to determine what sensitive data this new system handles, and how we want to mitigate the risks associated with it before making big picture changes.

While this is not an exclusive list of ideas and disciplines to minimize security risks, my hope is that this provides you with a line of thinking that you can apply not just to the security risk 'du jour', but also to other risks that haven't necessarily been realized yet by your practice and the ever changing landscape of security. ■

Ben Schmerler is a vCIO Consultant at DP Solutions, one of the most reputable IT managed service providers (MSP) in the Mid-Atlantic region. Ben works with his clients to develop a consistent strategy not only for technical security, but also policy/compliance management, system design, integration planning, and other business level technology concerns. You can follow DP Solutions updates on LinkedIn or their website: www.dpsolutions.com.

The Medical Practice Guide to Ransomware

WHAT YOU NEED TO KNOW TO KEEP YOUR PRACTICE AFLOAT

DP Solutions

MORE AND MORE, RANSOMWARE has emerged as a major threat to medical practices. Ransomware, a type of malware that encrypts data on infected systems, has become a lucrative option for cyber extortionists. When the malware is run, it locks victim's files and allows criminals to demand payment to release them.

Organizations of all types and sizes have been impacted, but medical practices can be particularly vulnerable to attacks. Ransomware is distributed in a variety of ways and is difficult to protect against because, just like the flu virus, it is constantly evolving.

There are ways to protect your practice against ransomware attacks. In this article you'll learn how the malware is spread and what you can do to avoid or recover from an attack. Hiding your head in the sand won't work, because today's ransom seekers play dirty. Make sure your practice is prepared.

RANSOMWARE TODAY

There are a few dominant types, or families, of ransomware in existence. Each type has its own variants and it's expected that new families will continue to surface as time goes on. Historically, Microsoft Office, Adobe PDF and image files have been targeted, but McAfee predicts that additional types of files will become targets as ransomware continues to evolve.

Once your files become encrypted by ransomware, cyber extortionists typically request payment in the form of Bitcoins or online payment voucher services to decrypt files. The standard rate is about $500, though we've seen much higher.

HOW RANSOMWARE IS SPREAD

Spam is the most common method for distributing ransomware. It is generally spread using some form of social engineering; victims are tricked into downloading an e-mail attachment or clicking a link. Fake email messages might appear to be a note from a friend or colleague asking a user to check out an attached file, for example. Or, email might come from a trusted institution (such as a bank) asking you to perform a routine task. Sometimes, ransomware uses scare tactics such as claiming that the computer has been used for illegal activities to coerce victims. Once the user takes action, the malware installs itself on the system and begins encrypting files. It can happen in the blink of an eye with a single click.

PROTECT AGAINST RANSOMWARE

Cyber criminals armed with ransomware are a formidable adversary. While medical practices aren't specifically targeted in ransomware campaigns, they may be more likely to suffer an attack.

Frequently, small medical practice IT teams are stretched thin and, in some cases, rely on outdated technology due to budgetary constraints. This is the perfect storm for ransomware vulnerability. Thankfully, there are tried and true ways to protect your practice against ransomware attacks. Security software is essential; however, you can't rely on it alone. A proper ransomware protection strategy requires a three-pronged approach: education, security and backup.

Education: Education is essential to protect your practice against ransomware. It is critical that your staff understands what ransomware is and the threats that it poses. Provide your team with specific examples of suspicious emails with clear instructions on what to do if they encounter a potential ransomware lure (i.e. don't open attachments, if you see something, say something, etc.).

Conduct bi-annual formal training to inform staff about the risk of ransomware and other cyber threats. When new employees join the team, make sure you send them an email to bring them up to date about cyber best practices. It is important to ensure that the message is communicated clearly to everyone in the organization, not passed around on a word of mouth basis. Lastly, keep staff updated as new ransomware enters the market or changes over time.

Security: Antivirus software should be considered essential for any practice to protect against ransomware and other risks. Keep all business applications patched and updated in order to minimize vulnerabilities.

Having antivirus installed isn't enough, it has to be kept up to date and it has to be enforced. Employees can't be allowed to put your company at risk by turning off protection. Additionally, restricting employees' ability to download malicious content, as well preventing malware from pulling down payloads from known bad servers is critical.

However, because ransomware is constantly evolving, even the best security software can be breached. This is why a secondary layer of defense is critical for businesses to ensure recovery in case malware strikes: backup.

Backup: Quality Managed Backup and Disaster Recovery (MBDR) services take snapshot-based, incremental backups, ideally hourly, to create a series of recovery points. If your practice suffers a ransomware attack, this technology allows you to roll-back your data to a point-in-time before the corruption occurred. When it comes to ransomware, the benefit of this is two-fold. First, you don't need to pay the ransom to get your data back. Second, since you are restoring to a point-in-time before the ransomware infected your systems, you can be certain everything is clean and the malware cannot be triggered again.

Cyber extortionists using ransomware are a definite threat to today's medical practices. However, a little bit of education and the right solutions go a long way. Make sure your employees understand what to watch out for and you can avoid many headaches. Never underestimate the dedication or expertise of today's hackers. They are constantly adapting and improving their weapon of choice. That's why you need top-notch security software and backup. Keep your practice safe and give your nerves a break.

To sum it all up, spreading knowledge among your staff and having the proper security software in place can help you avoid cyber-attacks. Patch management is essential. Be certain that your software is up-to-date and secure. In the end, it is backup that will help you pick up the pieces when all else fails. ■