HTA POST

Volume 5
Issue 9
September 2021

Healthcare Technology Advice for the Modern Independent Practice

WHAT'S NEW

September is National Preparedness Month. When I sat down to write this issue, I asked myself what that meant to me, my business, and my client's businesses. Preparedness could mean planting a garden, waterproofing a shed, insulating a window for winter, taking my dog to the vet, or planting trees. In IT security, preparedness can involve lots of technical buzzwords - cyber security, backups, disaster plans, policies, and procedures.

For me, being prepared isn't always about foreseeing every disaster and planning a response. It's thinking about the future that I want to see and laying the path to get there.

UPCOMING EVENTS

Wednesday, September 22nd	Kansas City MGMA *Caring For The Kingdom* Exhibit
In October: Wednesday 13th	*Back In The Game Of Healthcare* Annual MGMA Fall Conference

SEPTEMBER

S	M	T	W	T	F	S
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

See more at: *htadvisorsllc.com/events*

IN THIS ISSUE

Healthcare Technology Advisors

REFERRAL

Want to get up to $2,000 OFF your annual IT investment?

WIN a FREE iPad and EARN credits with HTA's Referral Rewards Program!

Learn more at:
htadvisorsllc.com/about-us/referral-program

This monthly publication is provided courtesy of Derrick Weisbrod, CEO, and the Healthcare Technology Advisors Team.

Our mission is to be trusted advisors guiding healthcare businesses through the complex IT and HIPAA landscape while providing a comprehensive service that always maintains a human touch.

RIGHT OF ACCESS STRIKES WITH ANOTHER FINE

The Office for Civil Rights (OCR) has been following its HIPAA Right of Access Initiative all year. The initiative was intended to support individual's rights to timely access to their health records, at reasonable cost, under the HIPAA Privacy Rule.

So far, many examples have arisen of health institutions simply not providing health records for years on end, usually only providing them once the OCR has begun an investigation. While the definition of "timely" may be flexible, when individuals are making decisions about health care, they need access to all the relevant information. In this country health care can factor into decisions about what job to take, where to move your family, or what school your child can safely attend. Life-changing decisions like this cannot wait years.

The most recent example comes from the Diabetes, Endocrinology & Lipidology Center, Inc. (DELC). A complaint was filed in early August of 2019 when the DELC failed to deliver the medical records of a minor to their parents in a timely fashion. Despite the law that requires them to provide the records, they did not fulfill the request until May of 2021 as a result of the OCR's investigation.

"It should not take a federal investigation before a HIPAA covered entity provides a parent with access to their child's medical records," said Acting OCR Director Robinsue Frohboese. "Covered entities owe it to their patients to provide timely access to medical records."

DELC has agreed to take corrective action and pay a $5,000 fine to settle their potential violation.

TECH TIP: WINDOWS 11 UPDATES

Microsoft has announced their upcoming operating system (OS), Windows 11, will be released next year. Much like the upgrade to Windows 10 some years ago, this upgrade will be offered for free to PCs that meet the minimum hardware requirements and are running the most recent version of Windows 10. The Windows 11 website will soon have a "PC Health check" available to let you know if your device can upgrade for free.

But why should you upgrade if your business is running happily on Windows 10?

The biggest reason to upgrade to the latest OS is security. With each iteration developers get better at building up safeguards and preventing cyber criminals from hacking into your networks. Security patches roll out regularly to fix loopholes and build up better defenses. Being on the latest OS means you have the latest defenses at your disposal.

Enhanced usability is also a perk of upgrading. Windows 11 will offer a refreshed look and new applications that make better use of modern technology. While this is largely a matter of preference, it may be worth upgrading if you find the existing Windows 10 experience unintuitive or clunky.

The last and most pressing reason to upgrade is the inevitable end of life of older versions of software. Eventually, Windows 10 will no longer be supported. This means security updates will no longer roll out, and the old versions will be vulnerable to cyber attacks.

Upgrading an office's computers is a daunting task. Make sure you contact your IT specialist to determine when the right time to upgrade is, and to make sure the job is done with minimal interruption to your practice's daily business.

SEPTEMBER IS NATIONAL PREPAREDNESS MONTH

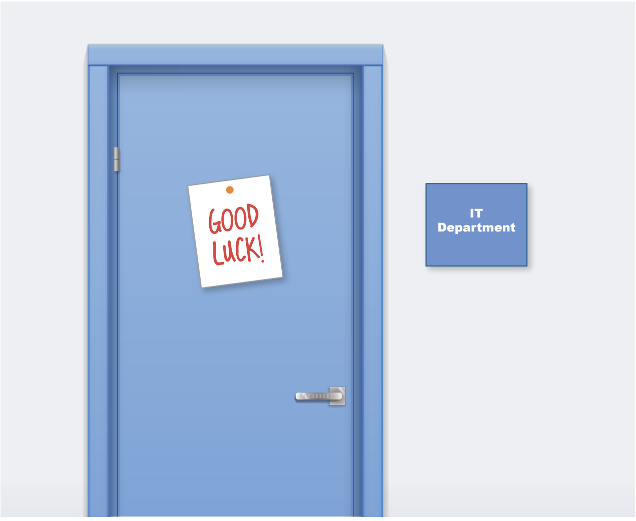
2020 was a banner year for cybercrime, and that trend isn't slowing down in 2021. In a recent survey, more than 35% of businesses reported double-digit increases in cyber attack threats including ransomware and nation-state threats. At the same rate, hiring people with security experience for in-house security is extremely difficult and costly, and risks are changing constantly.

How can you defend your healthcare practice effectively? One way to do that is by turning to the same thing that the big players are using: security automation. Today's smart tools enable companies to make a lean team more effective in spotting and stopping security threats. In fact, more than 40% of the organizations in IBM's most recent cyber resilience survey cited security automation as a major factor in their success at improving their cybersecurity posture.

Strengthening your security without a big spend is especially important in an era of burgeoning risk and shrinking budgets. In the same survey, researchers reported that choosing solutions that employ security automation can save more than 80% of the cost of solutions that rely on manual security. This is especially important for small medical practices that don't employ their own IT personnel. Being able to source cost-effective security is a monumental task, but one your IT company ought to be able to do with ease.

Most solutions that include security automation also include other powerful protections against cybercrime. Examples of these protections are: automated password resets that accompany multifactor authentication, single sign-on in a solution like IT Glue, and automatically delivered security awareness training from a solution like BullPhish ID. Today's strong solutions pack a punch that knocks out cybercrime; making security automation a smart choice for every small business and medical practice alike.

HOW DO YOU EXPAND YOUR IT TEAM WITHOUT THE OVERHEAD?



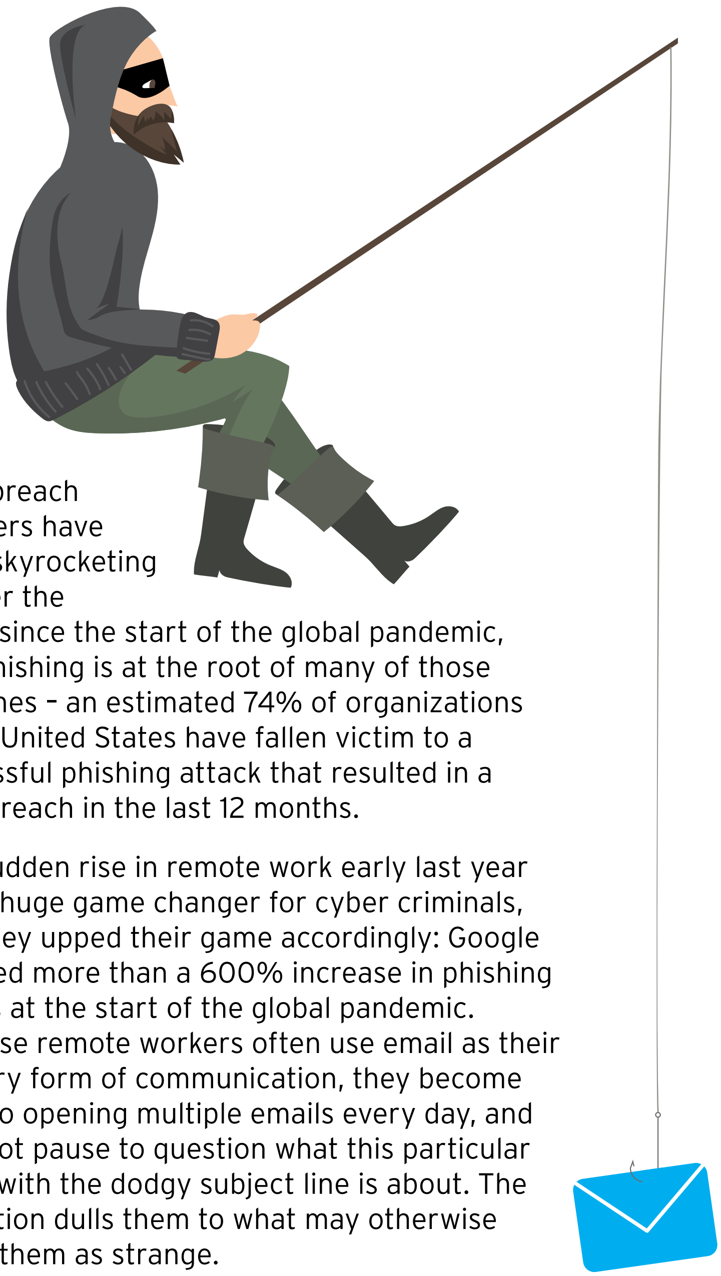
When your IT lead comes to you and expresses the need for more resources, how do you respond? Authorize overtime? Hire a new employee? Tell them good luck and hang in there?

There's an easy way to help your IT department do its job without the overhead of hiring a new employee. **It's called Co-Managed IT, or Co-MITs**.

Co-MITs is a customized set of ongoing IT services, support, and tools that we offer to companies with IT departments to help "co-manage" all aspects of IT support. Not only does this save your organization money (usually between 19% and 41%), but it also enables your IT team to be more effective and efficient, giving you greater peace of mind. You will also have better IT support and protections against downtime, cybercrime, ransomware, and IT-related compliance violations.

Putting in place this great add-on service for your IT team is an excellent first step in increasing your preparedness when it comes to the rising cybercrime threat facing all businesses.

PHISHING, DATA BREACHES, AND YOU



Data-breach numbers have been skyrocketing all over the world since the start of the global pandemic, and phishing is at the root of many of those breaches – an estimated 74% of organizations in the United States have fallen victim to a successful phishing attack that resulted in a data breach in the last 12 months.

The sudden rise in remote work early last year was a huge game changer for cyber criminals, and they upped their game accordingly: Google notched more than a 600% increase in phishing emails at the start of the global pandemic. Because remote workers often use email as their primary form of communication, they become used to opening multiple emails every day, and may not pause to question what this particular email with the dodgy subject line is about. The repetition dulls them to what may otherwise strike them as strange.

Would you open an email from Paypal saying your refund is being processed and you need to approve the payment? What about the ever-present "Verification Needed to Update Your Account." **More simply yet, would you open an email from your colleague who just left for a vacation, asking you to please print out this document and leave it on the Nurse's desk in the morning, because they forgot to do it?**

That's where social engineering comes into play. By posing as a member of your workforce (your colleague, boss, or employee), a hacker can trick you into doing something that seems routine and not at all dangerous. What you don't realize is that it isn't your co-worker sending that email. Their credentials have been compromised and a hacker is using their email account. They've attached a Word document for you to print out, something the hacker knows this person often does, because they've been able to look through their email history. When you go to open the document, you unknowingly download a virus onto your networked computer.

That's all it takes. That's how ransomware can infect your machine, your network, your entire building. That's how a hacker can gain access to your hard drive and servers, leading to data breaches. They can then leak protected health information or steal credentials and personally identifying information.

Where Do You Come In?

Unfortunately, even the best trained and most aware employees make mistakes – the single biggest cause of all cybersecurity incidents, including data breaches, will always be human error. A system like multi-factor authentication can stop 99% of password-based cyberattacks. Setting up this protection on your business devices will drastically reduce the risk of phishing attacks being successful.

You don't have to do it alone. Your practice can be protected with sophisticated password management, multi-factor authentication, phishing awareness training, and top-level cyber security. Our cyber security experts at Healthcare Technology Advisors can assist you in determining which solutions are a good fit for your practice and how best to implement them.

Call Healthcare Technology Advisors today and ask for a cyber health check-up. It's a great place to start.