April 2022

IT Radix Resource

We make IT work for you

What About IT?

What Your IT Department Should Know About Security

Professional managers of corporate information technology (IT) are responsible for being experts in their fields, leading their organizations forward especially in the areas of staff productivity and information/data security. Increasingly, these experts are recognizing the need to lean on outside experts to achieve their departmental and corporate goals.

"I don't know what I don't know." Some of the smartest managers of IT express that regularly. It may not sound astute, but it is. It acknowledges knowing a decent amount about a subject, but that there are knowledge gaps. They recognize their limitations and know that they cannot keep up with everything. So they engage in a practice called co-managed IT. Filling in information deficits, especially as it relates to IT security, may be the reason some organizations embrace this idea.

With constant news of security and data breaches and the ever-increasing risks, many organizations are exploring co-managed IT services, with a focus on cybersecurity. Our reliance on technology, the advent of cloud services, the work-from-home (or anywhere) movement and cybercriminals' increased access to any network from anywhere has caused this shift to more co-managed IT environments. Even a small data leak can result in enormous hazards to a small business. With so many users leveraging Dropbox and Google Drive, the likelihood of exposing sensitive information is increased, especially as the bad guys use ever more unique social engineering tactics to penetrate an organization and/or its network.

An outside resource focused on security will ensure that all your hardware and software is up to date with all necessary firmware updates and security patches. They will regularly monitor and audit all your systems ensuring that security and compliance standards are enforced. They will ensure your wireless network does not provide an open door to your core network. And they will provide endpoint security software solutions that are required by your business and expected by your clients.

Today, even more is expected and needed! A trusted IT resource will implement a 24/7/365 plan for threat detection and response. This is needed as cybercriminals do not just work 9 to 5, M-F. Recently, we have seen some major attacks occurring during 3-day federal holiday weekends. The vigilance of outside expertise cannot be undervalued.

(Continued on page 2)

Take Note

Duck Hunt
Join us for 10 weeks of duck hunting. All participants will receive a free webcam cover. More details on the back.

Microsoft 365 Pricing
Are you paying a premium for month-to-month licensing? Contact us for ways to save.

Celebrating Earth Day with Free E-Waste Recycling
Drop off your e-waste at our IT Radix office during the month of April between 10am-4pm.
Acceptable items here:
www.it-radix.com/recycling

If you would rather receive our newsletter via email, sign up on our website or send an email to resource@it-radix.com

More free tech tips at:
www.it-radix.com/blog

(Continued from page 1)

Additionally, security needs can change rapidly due to new threats or even the demands of a new client. Each may require a new or modified security solution. Managing that in-house requires significant ability to resource, plan and implement new methods very quickly. That can be difficult. An outside resource is far nimbler and making the change can be as simple for you as a change in a contract.

Beyond security, there is the need for outside resources when staff is too small or too busy and unable to take on a project of magnitude such as a cloud migration or an across-the-enterprise hardware/software upgrade. Advantages include: improved budget management, potentially lower labor costs as the need for an expansive internal IT staff is reduced, leveraging the experience of numerous outside IT experts, speedier exposure to and implementation of modern technology, faster ability to recover from a disaster, and lower IT risks across the board.

Stay tuned next month as we wrap up this security series and learn how to stop employees from leaking your corporate data.

Breaking **BAD HABITS**

Four Ways Your Employees Are Putting Your Business at Risk of Cyberattack

Your employees are instrumental when it comes to protecting your business from cyberthreats. But they can also become targets for hackers and cybercriminals, and they might not know it. Here are four ways your employees might be endangering your business and themselves—and what you can do about it.

1. **They're Not Practicing Safe and Secure Web Browsing.** One of the most basic rules of the Internet is to not click on anything that looks suspicious. These days, however, it can be harder to tell what's safe and what isn't.

A good rule of thumb is to avoid websites that do not have "https" in front of their web address. The "s" tells you it's secure—https stands for Hypertext Transfer Protocol Secure. If all you see is "http"—no "s"—then you should not trust putting your data on that website, as you don't know where your data might end up.

Another way to practice safe web browsing is to avoid clicking on ads or by using an ad blocker, such as uBlock Origin (a popular ad blocker for Google Chrome and Mozilla Firefox). Hackers can use ad networks to install malware on a user's computer and network.

2. **They're Not Using Strong Passwords**. This is one of the worst IT security habits out there. It's too easy for employees to use simple passwords or to reuse the same password over and over again or to use one password for everything. Or, worse yet, all of the above.

Cybercriminals love it when people get lazy with their passwords. If you use the same password over and over, and that password is stolen in a data breach (unbeknownst to you), it becomes super easy for cybercriminals to access virtually any app or account tied to that password.

(Continued on page 3)

(Continued from page 2)

To avoid this, your employees must use strong passwords, change passwords every 60 to 90 days, and not reuse old passwords. It might sound tedious, especially if they rely on multiple passwords, but when it comes to the IT security of your business, it's worth it. One more thing: the "tedious" argument really doesn't hold much water either, thanks to password managers like LastPass and Password that make it easy to create new passwords and manage them across all apps and accounts.

3. They're Not Using Secure Connections. This is especially relevant for remote workers, but it's something every employee should be aware of. You can find Wi-Fi virtually everywhere, and it makes connecting to the Internet very easy. A little too easy. When you can connect to an unverified network at the click of a button, it should raise eyebrows.

> "Education is a powerful tool and, when used right, it can protect your business and your employees."

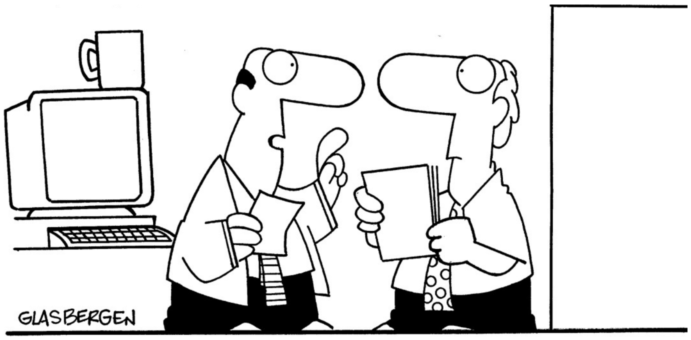
And unless your employee is using company-issued hardware, you have no idea what their endpoint security situation is. It's one risk after another, and it's all unnecessary. The best policy is to prohibit employees from connecting to unsecured networks (like public Wi-Fi) with company property.

Instead, they should stick to secure networks that then connect via VPN. This is on top of the endpoint security that should be installed on every device that connects to your company's network: malware protection, antivirus, antispyware, anti-ransomware, firewalls, you name it! You want to put up as many gates between your business interests and the outside digital world as you can.

4. They're Not Aware of Current Threats. How educated is your team about today's cybersecurity threats? If you don't know, or you know the answer isn't a good one, it's time for a change. One of the biggest threats to your business is a workforce that doesn't know what a phishing email looks like or doesn't know who to call when something goes wrong on the IT side of things.

If an employee opens an email they shouldn't or clicks a "bad" link, it can compromise your entire business. You could end up the victim of data breach. Or a hacker might decide to hold your data hostage until you pay up. This happens every day to businesses around the world—and hackers are relentless. They will use your own employees against you, if given the chance.

Your best move is to get your team trained and educated about current threats facing your business. Working with a managed service provider or partnering with an IT services firm is an excellent way to accomplish this and to avoid everything we've talked about in this article. Education is a powerful tool and, when used right, it can protect your business and your employees.



"Sports analogies are a powerful way to inspire teamwork, Fred. But next time use football, basketball or baseball—not duck-duck-goose."

Momentum NJ Magazine

Did you know that IT Radix is publishing our very own magazine dedicated to northern NJ businesses? Learn more about current technology trends and business concerns of local organizations like yours and about the growing cyberthreats targeting small and large businesses alike.

Momentum NJ
MAGAZINE
Maximize Sales, Profits, And New Clients By Classifying Your Leads
How Big Wins Are Secured By Managing The Minutiae
10 RULES FROM GEORGE FORMAN
On What It Takes To Reach the Top (and Stay There)
Page 12
IT Radix
This is a courtesy publication brought to you by IT Radix
Cathy Coloff, Managing Member of IT Radix

Contact us for your free copy of our first edition today!

"*Age appears to be best in four things; old wood best to burn, old wine to drink, old friends to trust, and old authors to read.*"

— Francis Bacon

Join Our Duck Hunt!

Spring has sprung and we invite you to participate in our "Duck Hunt" on our website for your chance to win a tablet.

Starting Monday, April 11, our duck target (pictured above) will hide on a different page of our website each week.

It's simple: Find the duck hidden somewhere on our website, click on the image, and enter your name to win.

Only one entry per person per week will be accepted, but be sure to enter once a week to increase your chances of winning. We'll draw the winning name on the last day of spring, Tuesday, June 21.

From the desk of Cathy Coloff

Time for some target practice…

Cathy

If I had invested a hundred dollars every time someone I spoke with about cyber risks said that they had nothing of value or interest, I'd be a wealthy gal. So many assume that they do not have to worry about cyber risks and put little-to-no thought into protecting themselves or their organization. I still find this to be true even after the cyber incidents publicized in the news and more. Sadly, these organizations may find themselves to be an easy target for cyberattacks in the future.

Good cybersecurity requires discipline, good habits and practice recognizing and reacting to cyberthreats. Cyber criminals routinely hunt for easy targets to exploit.

While we never want anyone to be an easy target for a cyberattack, we thought it might be fun to flip the roles and give you an easy target to find on our website. Read more below about our online "duck hunt"—find the sitting duck and at the same time, learn how you can keep cyber "cwiminals" at bay.

On the Road to New Adventures!

An interview with COO, Marybeth Smith:

IT Radix: What sparked your desire to go on a road trip?
Marybeth: When our youngest went off to college last fall, we used it as a great excuse to take a road trip to California and Oregon.

IT Radix: What did you like most about your road trip?
Marybeth: It was remarkably freeing to set out on an adventure and see something new every day. Our itinerary was totally flexible and allowed us to experience different vibes along the coast. We traveled through groomed Sonoma wine country, the redwood groves of the Anderson Valley, the wild coast of Mendocino, the winding canyons and rolling hills of Willamette Valley, the deserted Oregon Coast and finally the funky neighborhoods of Portland.

IT Radix: What was your favorite experience?
Marybeth: Learning about wine tasting! I had never done an in person tasting before. Most interesting was that glassware—size and shape—has a huge impact on how the wine tastes. Try it!

For Marybeth, it was ultimately about the journey… the laughs and memories made along the way.