February 2022

IT Radix Resource

We make IT work for you

Take IT From the Top!

What Your CEO Needs to Know About IT Security

A week does not seem to go by without breaking news of a new data security breach affecting numerous, well-known organizations in the United States. This fact alone has made information technology an important functional area of any business entity. So, it is now incumbent upon any Chief Executive Officer (CEO) to stay on top of all aspects of the information technology roles in their organization, especially as it relates to data security. Technology permeates every aspect of a business, and IT must be managed from the top!

Historically, the role of technology or "IT" staff was to facilitate increased staff productivity. The advent of advances in cloud technology and the widespread access to low-cost internet allow cybercriminals to wreak havoc from across the street or across the globe. This means that data protection, privacy and security are now more important than ever to the IT professional. The regrettable truth is that a major cyber breach could result in the loss of proprietary and/or confidential information that could result in a business losing important sales revenue streams, exclusive intellectual property, and enormous profits—as well as its reputation. All too often the worst case happens and the organization does not survive.

The Outside Threats. C-Suite managers have read and been presented with a host of security recommendations in great detail. These include everything from a patch management regimen to firewall and backup software/ hardware to external auditing and testing…and the list goes on!

The Weakest Links Are Inside. Security precautions are put in place by IT staff to reduce the threats from hackers, adversaries, competitors and the like, but the weakest links reside inside the organization and relate to the internal corporate staff. Some examples of security precautions include: an employee's unsecure home/remote network potentially due to a game device used in the home by a child; a laptop stolen or left at an airport screening area; staff sharing sensitive corporate data on cloud-based services such as DropBox that do not have adequate security measures in place; a disgruntled colleague expressing his/her anger by going outside security policies and sharing key data in an external environment. The list can go on and on. The CEO must pay attention to these and other internal

(Continued on page 3)

Take Note

February 2
WEBINAR

Back By
Popular Demand

30-Minute Tech Talk:
Advanced Security Solutions (Take 2)
www.it-radix.com/webinar
Starts @ 12:10pm sharp

RED Month E-Waste Results
IT Radix collected and properly recycled 901 pounds of e-waste during our November RED Month.

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

Digital Disruptions on Remote Workers

The risk of cyberattacks grows with more people working from home. In 2020, between the months of March and July, nearly half of all businesses dealt with some sort of digital disruption. Some of the most common were:

Worker Productivity Losses. When hackers infiltrate company computers, they might steal employee identities. This will hurt your business indirectly as workers have less time for work while they grapple with their identity being stolen.

Internet-of-Things Infiltrations. Since "smart" devices can be hooked up to a central server, there are more avenues for hackers to gain access to sensitive company data.

Ransomware Attacks. Businesses of all sizes are falling victim to ransomware attacks, but it's the small- and mid-size ones on a tight budget that really suffer from the fallout.

Stop these kinds of attacks by educating your workforce on best practices for avoiding hackers and make sure their systems are up to date with good cybersecurity software.

IT Radix is here to help!

Proudly folded & stuffed by Central Park School

Introducing… Patrick Postiglione

Patrick got his start in IT at Anthem Institute of Technology where he received training in Network Administration and PC Support. With over 22 years of professional IT experience, Patrick has worked in a variety of end user hardware, software and help desk support positions. Most recently, he worked as a Sr. Support Engineer for an office technology company prior to joining the ranks of our IT Radix team.

As an IT Consultant at IT Radix, Patrick wears many hats. He provides on-site support for one of our clients two days a week and is the primary technical contact for another providing automated onboarding/offboarding and technical inventory support. His daily activities include hardware/software troubleshooting, server maintenance, workstation configurations and supporting clients with their day-to-day technology issues. Patrick is an effective communicator and excels at being able to explain IT issues in easily understood layman's terms.

Patrick's favorite quote:
"The world ain't all sunshine and rainbows. …it ain't about how hard you hit. It's about… how much you can take and keep moving forward. That's how winning is done!" – Rocky Balboa

Growing up in West Orange, Patrick is back to living in his childhood home while helping his mom downsize and relocate (not an easy task). When not working, Patrick enjoys visiting museums with a big interest in history (especially U.S.), politics and anything tech related. He likes reading sci-fi and westerns (Cormac McCarthy is his new favorite author) and playing video games (first-person shooters and RPG). An all-around movie buff, Patrick enjoys all genres of movies and is quick to quote from his favorites. Check out the snippet of his favorite quote above. 😉

Patrick's personal philosophy: Wisdom over intelligence

Free Cybersecurity Audit Offer

At no cost or obligation, our highly skilled team of IT pros will conduct a cybersecurity audit for new clients to uncover loopholes in your company's IT security.

After the audit is done, we'll prepare a customized report that will reveal specific vulnerabilities and provide an action plan for getting these security problems addressed fast. Schedule your cybersecurity audit today: **www.it-radix.com/cybersecurity-audit**

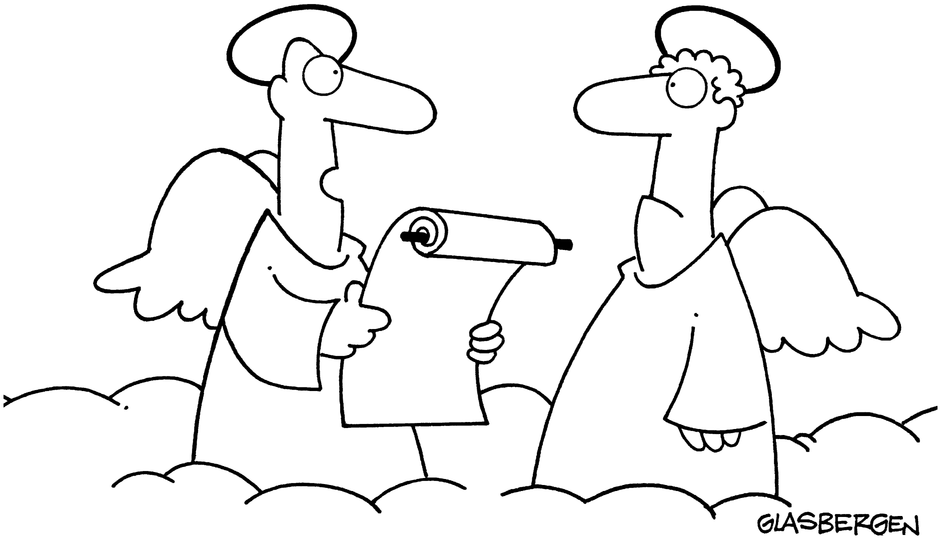
(Continued from page 1)

threats and establish policies that are communicated, enforced, and updated. They should include an ongoing staff cybersecurity training and testing program to reduce these risks.

Questions to Ask. Whether relying on internal or external resources to manage the IT role in an organization, top management must consistently ask these questions to keep the staff on top of things: What is the current risk level and business impact of a cyberattack to our company? What is the communication and action plan in case of any breach? What industry standards exist for our organization and how do we compare to those standards? What is our cybersecurity insurance posture and is it adequate? When did we last execute a cybersecurity risk assessment and what were the recommended outcomes and tasks? What is our overall cybersecurity and disaster recovery plan including prevention, resolution, and remuneration?

Lead by Example. Successful CEOs lead by example and keep important issues top of mind. Be sure to consistently remind all employees of the importance of cybersecurity and their role in minimizing risks. Stay informed and vigilant. Never trade convenience for security. Leverage the expertise of your team and you will succeed!

Stay tuned next month as we shine a light on your COO and share what he/she needs to know to keep your corporate data safe and secure.



"...and you spent 5.73 years of your life deleting spam from your e-mail."

Archiving Your Email

So much of the business we conduct in today's corporate landscape is digital. According to Osterman Research, as much as 75% of your company's intellectual property is contained within your email and messaging programs. At IT Radix, "Backup" is our middle name, but another tool we recommend for securing your important communications is Email Archiving.

Email Archiving may already be familiar to you… it has been a useful storage management aid for years. However, its benefits go beyond the ability to manage the space your emails take up. All industries face compliance rules, and Email Archiving is designed to manage that. Having Email Archiving in place also ensures you are prepared in the event of an audit by indexing and retaining every email in and out of your mail server.

Thanks for the referrals!

Referrals are the best form of compliment! We would like to thank the following for referring us to their friends and colleagues:

Lewis from My Tech Guy
Lisa from Paymedia
Liz from Third Pole Therapeutics
Marissa from Esposito's Electric
Mike from Prime Pensions, Inc.
Ron from Innovative ISP

Visit us at www.it-radix.com to learn more about our Referral Rewards Program!

> "Cherish your human connections—your relationships with friends and family."
>
> — Barbara Bush

security TIP of the month

Set Up Bank Alerts!

Why? Most banks will send you an email alert whenever money is withdrawn from your account via check, debit card or transfer. Setting up those alerts will allow you to spot and report fraudulent activity BEFORE the money has been siphoned into the hands of a cybercriminal. Doing this just might save your bacon!

Contact IT Radix for more tips on staying safe online!

From the desk of Cathy Coloff

Cathy

Growing up in Cary, NC, we didn't often have snow days; but when we did, it was great! No school for several days because the area simply wasn't prepared for snow removal since it occurred so rarely. I wish cyberattacks were as rare as those snow days of my youth. Sadly, several of our clients were the victim of cyberattacks, ransomware, email hijacking and more in 2021—and there's no end in sight.

As the Managing Member of IT Radix, I am constantly reminding our team to be vigilant in evaluating and implementing new security measures and training and testing our team on a regular basis. I want IT security to be as automatic as putting on your seat belt when you get in your car. Unfortunately, security isn't always convenient, and it's tempting to skip it. My advice—don't! As one client experienced, paying out a half million ransom to keep their data off the Dark Web is not fun and definitely not good for business.

Mom always said to put something on your head to keep warm outdoors in the winter. Now it's time to put on your IT security hats and keep your organization safe from cyberattacks. We can help you get outside and enjoy a snowball fight with the kids knowing that your IT security measures are protecting your team and your business assets.

Chillax With Winter Camping

An interview with Treasurer, Doug Verge:

IT Radix: How were you introduced to Winter Camping?
Doug: Thirty or so years ago when I was in college, my roommate thought it would be a fun thing to do. So, off we went! We have carried on the tradition of Winter Camping every year since.

IT Radix: What do you like most about Winter Camping?
Doug: What's great about Winter Camping is the peace and solitude. You don't have to worry about rain or bugs; and without leaves on the trees, you can see for miles around you. Winter camping does require specialized gear: a sleeping pad which serves as an additional layer of warmth between your sleeping bag and the snowy ground, winter tents which can withstand heavy wind and snowfall, and other items like snow shovels, camping stoves, snowshoes, and skis.

IT Radix: How does this experience enhance your life?
Doug: Winter campgrounds are sparsely occupied, quiet, and offer an opportunity to get away from the stress of everyday life.

As for Doug, Winter Camping is a cool way to chillax and unwind.