October 2022

IT Radix Resource

We make IT work for you

Assess Your Risk and Plan for IT

Was your organization ready to work under the conditions created by the pandemic? If you had done a risk assessment, you were likely more prepared than others—even if a pandemic wasn't something you included as a high probability risk.

A risk assessment is a process where you identify the hazards that could negatively impact your organization's ability to conduct business.

Equally important, you'll identify measures, processes, and controls to reduce the impact of these risks.

Here's an overview of the steps:

Step 1: **Identify the hazards or risks to your business.**
These could include natural disasters, utility outages, supply chain storage, and cyberattacks. We have a template to get your juices flowing.

Step 2: **Determine what or who could be harmed.**
Business assets that might be at risk include business operations, IT systems, or even employee safety.

Step 3: **Evaluate the risks and develop control measures.**
At this point in the process, you'll want to identify both the impact and the likelihood that the hazard will occur. This process will help prioritize which control measures to put in place first to eliminate or reduce the impact on the organization.

Step 4: **Record your findings.**
It's important to document the risk assessment findings and control measures in a place that is easy to find in the event something occurs.

Step 5: **Review and update your risk assessment regularly.**
Things change rapidly. Smart organizations are alert and flexible and are able to pivot and adapt.

(Continued on page 2)

Take Note

October is Cybersecurity Awareness Month
Combat cybercrime!
Ask us about our Security Awareness Training and advanced security solutions.
And… participate in this month's security webinar.

October 26
WEBINAR
10-Minute Tech Talk:
Mistakes You're Making on IT Security Questionnaires
www.it-radix.com/webinar
Starts @ 12:10pm sharp

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

Assess Your Risk and Plan for IT

(Continued from page 1)

Don't rely on the roll of the dice when it comes to accessing potential risks to your organization. Be proactive and plan for IT!

Need help putting together your organization's risk assessment? Call IT Radix today!

We'll be happy to help you get a handle on your potential business risks and put good technology solutions in place to minimize or manage your exposure and keep your organization moving forward today.

Proudly folded & stuffed by Central Park School

Introducing… Lynn Ferraro

Lynn is currently attending Southern New Hampshire University working towards her bachelor's degree in Business Administration. She plans to graduate next month, and we are so excited for her!

Lynn came to IT Radix with over 30 years of office experience having worked in a variety of office administrative and customer service settings. Having an eagle eye for details, Lynn often found herself being the "go to" person in her past roles.

As an Office Manager at IT Radix, Lynn is the "Jane of all trades" and does a little bit of everything to make our day-to-day office operations run smoothly behind the scenes. She often refers to herself as the "Happiness Coordinator" 😉 and enjoys planning special activities for our staff promoting positive morale and team building. After all, one of our Core Values is "We Have Fun!" A strong team player, Lynn excels at multitasking and problem solving. Her overall positive attitude and outlook is a wonderful addition to our team.

Lynn's favorite quote:
"Do the best you can until you know better.
Then when you know better, do better."
— Maya Angelou

Born and raised in northern NJ, Lynn now resides in Passaic County. When not working or taking on-line college classes, Lynn is busy with her side business selling makeup, fragrance, and skin care products. She enjoys de-stressing and rejuvenating with yoga and long walks around her neighborhood as well as spending quality time with her adult children, Kate and Alyssa, and boyfriend, Chris.

Lynn's personal philosophy: Life is short, so enjoy each day. Live each day like it's your last.

Cyber Intelligence: A "Duck" Tale of Two Incidents

Cyberattacks are one of the biggest threats that businesses face today. One popular tactic, spear phishing, is on the rise, so be alert!

Spear phishing is the act of sending emails from a known sender's name to increase the chances of the recipient trusting and opening the email and taking action that unintentionally hurts the organization. Cybercriminals often target all levels of employees from low-to-mid level employees in addition to management level—anywhere they think they can make an inroad. It is important to train all employees about spear phishing cyberattacks because **88% of all data breaches are caused by employee actions.** Requiring that ALL employees participate in security awareness training significantly reduces the chances of an employee-caused attack.

Are you well positioned against a targeted cyberattack? Let's review two recent incidents.

Incident #1: Headed for Disaster

"Sitting Duck Partners" came to us concerned they were victims of a spear phishing attack. This company was very susceptible to the attack because they had not taken the steps to keep their company safe. Their two biggest mistakes: Their employees were not educated on how to identify emails that can be a threat to their company, and they did not use Multi-Factor Authentication (MFA). They were a prime target for a phishing email. By not being prepared for an attack like this, "Sitting Duck Partners" not only gave the criminals $150,000 but had to deal with other repercussions, including increased stress, and loss of days of productivity within their business.

Incident #2: Taking the Right Approach

Contrast this with "All Our Ducks In A Row, Inc.", who came to us saying that they think they were targeted by a spear phishing email. Thankfully for them, their employees were trained on how to recognize a suspicious email, making the spear phishing attack unsuccessful. The staff member who received the email, immediately raised a red flag, and deleted the email. Choosing to train their employees on how to utilize things like strong passwords, MFA, and equipping them with knowledge of how to identify the different types of threats such as phishing emails was key to the protection for "All Our Ducks In A Row, Inc."

Keeping your employees up to date on trending cybercrime tactics plays a huge part in keeping your company safe from becoming a victim of a cyberattack. IT Radix offers cybersecurity training geared to your company's specific needs. Contact us today to learn more about our employee cybersecurity training and testing.

Social Media Sharing Can Be Risky Business

Sharing too much information online can be extremely harmful to your online security.

When you fill out an online Facebook quiz, you may be unknowingly sharing your personal information with cybercriminals. It may seem all fun and games—comparing answers among Facebook friends—but these quizzes often ask questions like where you went to elementary school, what your first car was or the name of your first pet.

Often, these same questions are used for verifying password resets or as the security questions to log into an account. Don't pave the way on social media for cybercriminals to access your accounts.

Mum's the word when it comes to staying safe online.

Welcome!

A warm welcome to our newest Management and Support clients:

GHS Philanthropy Management
SMS Security Systems, LLC

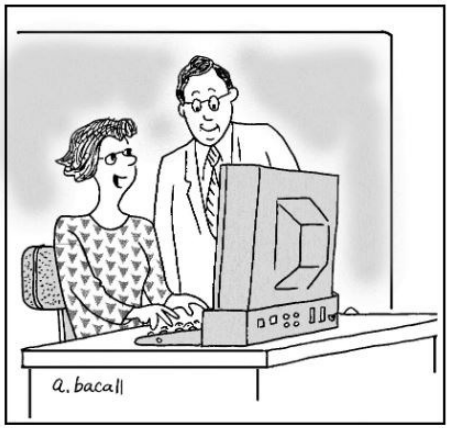
Remember, IT Radix is here to service all of your technology needs!

IT Radix
We make IT work for you
49 S. Jefferson Road
Whippany, NJ 07981

Inside This Issue

IT Radix Family and Friends
321 Delighted Clients Boulevard
Geekville, NJ USA

"Life is a journey to be experienced, not a problem to be solved."
— Winnie the Pooh



"My password is 'Again.' Whenever I forget my password, the computer says, 'Try Again.' "

From the desk of Cathy Coloff

This newsletter issue focuses on risks and cybersecurity incidents from a business perspective. As a mom, I've had to think about and address our risks at home, including cybersecurity. I was surprised at how quickly my son encountered the pitfalls that come along with technology. He easily circumvented the restrictions imposed by parental controls with a quick Google search. With the proliferation of Internet of Things (IoT), I've had to think about whether I really want to be able to open our garage door remotely.

Sadly, most don't think about these cybersecurity risks but rather, embrace the convenience and ease that IoT technology brings to their lives and homes. Don't get me wrong, I like that too. However, I'm not willing to take the risk—my doors being unlocked without my knowledge, our security camera being used to access my home computer and all that I access from it. No thanks!

COVID has forced many organizations to embrace work-from-home or remote working, but what risks and security exposures from their team members' home networks have they created? We've already seen incidents of a remote worker introducing ransomware into the corporate network and cloud storage. I'm sure there's more to come. October is Cybersecurity Awareness Month. Consider the new risks working remotely has introduced to your organization and ensure that you've put some minimum-security measures in place. Keep the cyber ghosts and goblins at bay and enjoy Halloween with costumes and candy as it was meant to be!