IT Radix Resource
We make IT work for you
March 2018

The Game of Life

Strong IT Security Policies Reduce Your Risk

Have you ever played the game of *Risk*? If so, then you know the object is to take control of and occupy every territory—thereby eliminating the other players. In business, one could say that your "territories" are your assets which includes technology. While we don't think the goal in business is to eliminate the other players, sadly, there are a variety of other players in the world who wish to take control of your "territories"…both good and bad. Having strong IT security policies can reduce your risk and help you succeed at your business goals.

As it turns out, many (dare we say most?) small-to-medium size businesses do not have even basic IT security measures in place, much less written policies. Just like in the game *Risk*, you need to control your entire organization, watch your borders for upcoming attacks, and have a variety of defenses in place to protect your business. As an example, the various strains of crypto or ransomware viruses attempt to take over your data and encrypt it for ransom. There is no magic bullet to prevent this type of attempt on your data. But rather, it is a collection of policies that are implemented and followed that can help your organization avoid being a ransomware victim. Multiple layers of defense are necessary that start with recognizing the threats, identifying where critical information lives and then taking steps to protect it.

Your IT security policies should cover all aspects of your IT environment which includes often overlooked devices such as printers and employee-owned smartphones or services provided by third-party vendors.

As in the game of *Risk*, creating and enforcing IT security policies requires diplomacy. The human element is one of the biggest risk factors when it comes to IT security. It's important to develop policies that are easy to understand and easy to follow and enforce. Additionally, everyone in the organization needs to be educated just like everyone needs to know and understand the rules of a game. Of course, wherever possible, IT Radix encourages your organization to implement solutions that automate security as much as possible. However, it's impossible to implement automatic solutions to fully protect your organization; hence, the heightened emphasis on educating your team about IT security. To help evaluate how well your policies are understood and followed, we encourage you to periodically test your team. It's easy to get complacent—consistent reinforcement and testing helps mitigate this concern.

Your IT security policies should cover all aspects of your IT environment which includes often overlooked devices such as printers and employee-owned smartphones or services provided by third-party vendors. With the advent of the Internet of Things (IoT), we're finding the scope of IT policies is expanding even further to include areas such as HVAC environmental controls, physical security and more. IT Radix has helped a number of our clients to develop and document these policies often in response to audits that our clients are undergoing or as

(Continued on page 2)

10TH ANNIVERSARY 2008 - 2018

What's New

March 23
Client Appreciation Pancake Breakfast
Come enjoy a presentation on *Email Encryption* and *Two Factor Authentication*, visit with our IT Radix staff and build business relationships with other IT Radix clients.
www.it-radix.com/appreciation

March 31
World Backup Day
Avoid a potential disaster and back up your data files!

Welcome Laurie
We'd like to extend a very warm welcome to **Laurie Sloane** to our Service Coordination team—another friendly voice behind our phones.

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

Stick with Us and You Won't be Sorry!

The title of the board game, *Sorry!*, comes from the many ways in which a player can thwart the progress of another, while apologetically saying, "Sorry!" That may be all fun and games, but when it comes to businesses who don't have an IT management and support plan in place, there's only so much you can do to reactively fix a disaster. And, sometimes "Sorry" is all that can be said. "It's a sad, sad situation," concludes Elton John; and "sorry seems to be the hardest word."

Such is the case a local business experienced recently. They came to us panic-stricken when their server crashed. They were legitimately concerned since there was critical company data stored on this server in a SQL database. To make matters worse, there was no backup drive connected. Their server was a significantly older piece of hardware still running Windows 2003 operating system (which is no longer supported by Microsoft). The truth of the matter is that hardware fails all the time (hardware actually has a shelf life). In the end, the only option they had was to keep their fingers crossed and bring the drive to a firm that specializes in recovering data from broken hardware.

If they were an IT Radix management and support client, this never would have happened! We take a proactive approach to monitor AND maintain your network and computers to prevent problems before they happen. We keep an eye on the status and general health of your computer systems 24/7, each and every day. With our remote monitoring tools, we can detect and prevent the vast majority of potential IT issues—BEFORE they happen. The issue of running an old, unsupported operating system would already have been addressed, since we keep your network and computers current with the latest software updates, anti-virus and critical security patches. We don't rely ONLY on automated tools. Every month, an experienced tech professional reviews your computers and network from soup-to-nuts—we call it Proactive Maintenance and it's designed to supplement our state-of-the-art tools.

Key components of a healthy computer network are included in all our plans:

- Reliable backup of all your critical business data—both a local image backup (easy to retrieve and recover) and a second data backup in the Cloud for added offsite protection
- Backup monitoring and testing
- Anti-virus software and updates
- 24/7 alerting to potential issues

Our IT Radix Management and Support plans are *Hands Down* the best assurance to give you peace of mind. Stay out of *Trouble* and avoid getting a *Headache*! Stick with us and you won't be *Sorry!* (Excuse all these board game references; we couldn't resist!) But, in all seriousness, give IT Radix a call today and let us make IT work for you!

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:

Bill from AccountingDept.com
Joe from Yodice & Company CPAs
Lisa from New Jersey Builders Assoc.

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

Strong IT Security Policies Reduce Risk

(Continued from page 1)

a result of some type of security incident. To simplify the process, we leverage pre-existing templates that are then modified to reflect our clients' actual IT environment. While it's tempting to adopt someone else's IT security policies, we often find that our clients are unable to actually enforce or implement some of the items within these adopted policies.

Increase your chances of winning the game of *Risk* by proactively creating your own IT security policies today. We're here to help!

OUR CLIENTS SPEAK OUT:

THE BUZZ

"Provention Bio, Inc. is a virtual international clinical-stage biopharmaceutical company dedicated to sourcing, developing and commercializing novel therapeutics and cutting-edge solutions to intercept and prevent immune-mediated disease. As such, we are utterly dependent upon information technology to create and manage our mission-critical virtual infrastructure and multiple network interfaces and communication pathways. IT Radix has helped Provention design, build and maintain our architecture and day-to-day operations. IT Radix's service levels are ***exceptionally high****, and from our perspective,* ***well-tested****. IT Radix has more than earned its status as a* ***strategic partner*** *contributing substantially to our corporate cooperative and distinctive capabilities. We would recommend and endorse IT Radix without hesitation."*

Ashleigh Palmer, CEO— Provention Bio

Step 3 to Enhancing Your IT Security

Are your employees' personal smartphones connected to your business network? They are 100% up to date, right? Unsure? **Mobile technology is a prime target** when it comes to security.

Protect your network by implementing technical solutions to "sandbox" your mobile devices or enforce your organization's mobile device security policies.

One simple step is to create a guest Wi-Fi network, and do not share the internal Wi-Fi network password with anyone. A good additional layer would be security software installed on the mobile device itself. In 2016 alone, malware attacks nearly doubled to 8.19 billion—primarily targeting Android's ecosystem.

Call us today to learn how to "up" your game when it comes to mobile security.

Proudly folded & stuffed by Park Lake School

SPECIAL OFFER

Not All Fun and Games!

Sign up for IT Radix's Dark Web monitoring service during the months of **January, February** and **March**, and get the 1st month of monitoring service free.

Visit IT Radix at www.it-radix.com to learn more about our services!

Mastermind: Inside the Mind of a Hacker

Cybersecurity is finding its way to the center of every business owner's radar—and if it isn't, it probably should be. Consider the companies we know (and trust) with our confidential data. All seems well until suddenly they're the victim of a massive cyber breach. Who ever thought Merck or Equifax would end up making headlines for data breaches, with millions of dollars lost as a result? How is it that hackers work as fast as they do?

Back in 1970, a board game known as *Mastermind* was released. The game is played between two opponents: The codemaker and the codebreaker. The codemaker creates a sequence, and it's up to the codebreaker to solve the code in the least amount of terms possible.

Hackers are expert game players. In the case of your computer, the key to the code is usually your login credentials (user name and password.) Once they have those, they have cracked the code. Here's a list of some of the most common, and most effective exploit techniques:

Phishing – The vast majority of data breaches happen when an employee is taken advantage of by a scammer posing as a legitimate person. Phishing attacks are bogus emails that can do serious damage if your staff is unaware (e.g., an email that poses as Microsoft and asks for login credentials to "update" your software.) It is easy for an unwitting staffer to provide access to their email account.

Vishing – This is another form of phishing; however, this time it's a phone call. Phony callers engineer a fake caller ID or local phone number to create trust. A website can mimic Microsoft or other trusted resource. Either way, you are tricked into providing your login credentials or other confidential information. Another example of vishing is a web-site that freezes your computer and says: Call 1-800-Definitely-Not-A-Scam-Now to fix your machine. Users who aren't trained on what to watch out for click into this and open their computer to the hacker…inadvertently risking your company's revenue, reputation, and in some cases, your business. And, to make matters worse, if employees have work credentials or information on a personal device, what happens out of the office can also impact your business.

Keylogging – After the intruder has snuck onto your machine with these codebreaker techniques, they can continue to break through layers of your code. Malicious programs to track your employees' keystrokes are installed so that the hacker can see your account-ing passwords (or worse, your clients' accounting passwords). Then, the attacker simply bides their time, until they have everything they need to compromise your network.

So, what can you do to stop this from happening or at least greatly reduce your risk? Educate your team on what to look out for. The #1 reason for data breaches is a user accidentally giving away "code" secrets to the codebreaker. You want your team to be savvy and cautious. And, you want passwords to be high quality and different from personal passwords. The latest password wisdom says that a random phrase, with a combination of letters, numbers and characters is the best approach.

Once the codebreaker has their foot in the door, it's far too late. Their automation techniques can do everything from holding your data hostage for a ransom, copying themselves on every email you send, and intercepting the messages you receive. **Seriously, folks, this happens more than you'd think!**

Our advice? Encourage your employees to take advantage of the security and training resources available to you through IT Radix. We realize security is a big topic. It's not always easy to get started; but luckily, you don't have to figure it out alone. Give us a call. We've got your back!

"We don't stop playing because we grow old; We grow old because we stop playing."

— George Bernard Shaw

"Right now we're only hiring twins. One for the office and a back-up copy for the cloud."

From the desk of: Cathy Coloff
Subject: March Kicks Off Our 10 Months of Giving Back!

2018 is IT Radix's 10-year anniversary. We're excited to share this important milestone with our extended IT Radix family. *Give Back* is one of our core values; and to that end, we are pleased to celebrate our anniversary with **10 Months of Giving Back** beginning this month. We're kicking off the celebration by supporting National March Into Literacy Month and collecting books to support Literacy Volunteers of Morris County. The books can be either new or gently used. Would you like to help us celebrate? Stop by our office with your book donations any day this month.

Also in March, we have another reason to stop by our office on March 23—our annual **Client Appreciation Pancake Breakfast**. We'll be feeding your body and your mind with yummy food and information on two important security technologies that most organizations should have in place today. Come see how easy *Email Encryption* and *Two Factor Authentication* can be and how it can benefit your business' IT security. (Visit our website for more details.)

I'd like to round out the month with a reminder about a very important IT holiday—**World Backup Day**! Let's face it, technology isn't perfect, which is why a reliable backup is your best friend. Everyone needs a data BFF!

Give us a call today! We'd be happy to review your backup because IT Radix has got your backup!

Gaming Fun Facts!

- *Jenga* is Swahili for "build."
- The longest game of *Monopoly* lasted 70 days.
- *Chess* originated in Eastern India around 280-550 A.D. The original pieces (infantry, cavalry, elephants, and chariotry) eventually became pawns, knights, bishops, and rooks.
- Talking is not permitted during a game of Chess. It's not required to announce "check," only "checkmate."
- In 1984, Fred L. Worth sued for $300 million because more than 25% of *Trivial Pursuit*'s questions were lifted from his books. He lost because facts can't be copyrighted.

Monopoly: A Force for Good

Did you know that the board game, *Monopoly*, helped POWs escape? Or, that it helped a children's hospital become $1 million dollars richer? Truth be told, the game of *Monopoly* has been used to help society...

During World War II, the Nazis allowed British prisoners to receive care packages from humanitarian groups like the Red Cross while they were in prison. Armed with this knowledge, a British Intelligence Officer devised a plan to help POWs escape. They worked with the *Monopoly* manufacturer in Britain to hide tools for escape within the game itself. Tools were hidden such as: real money amongst the *Monopoly* play money, magnetic compasses, metal files and a folded silk map (which wouldn't become worn or dissolve in water). Soldiers were instructed that if captured to be on the lookout for Monopoly games sent in care packages. The plan worked like a charm! Of the 35,000 British soldiers who escaped imprisonment during World War II, it is estimated that some 20,000 of them used these silk maps, compasses, and assorted tools. Talk about a get out of jail free card!

For over 25 years, McDonald's has run a *Monopoly*-branded promotion in which each of its products has a game piece that corresponds to a square on the classic *Monopoly* board.

In 1995, St. Jude Children's Research hospital received an anonymous gift of McDonald's pieces worth $1 million. Even after McDonald's realized that the pieces had been embezzled, they still honored the donation to help sick children.

Through the years, *Monopoly*, has become a force for good!