March 2022

IT Radix Resource

We make IT work for you

Become a Smooth Operator

What Your COO Needs to Know About IT Security

The Chief Operating Officer (COO) role is a tough one and often misunderstood. Modern business literature says that while no two COO positions are the same, there are some guiding principles for all: (1) identify key issues and opportunities for the organization, (2) align the firm and leverage all areas of consensus, (3) attract and retain top talent, (4) drive the strategic planning process, and finally, (5) create a culture of constant improvement.

That is a substantial set of things for one role to be concerned about! In today's environment, a key area of importance, focus, and concern for the COO is the Information Technology used in the business—specifically, the security and protection of that data. To become a "smooth" COO who minimizes cybersecurity risk, below are some important considerations.

Governance: Establish a cybersecurity policy that conforms to all legal and industry guidelines and standards. Define roles and responsibilities throughout the organization for all security matters. Ensure that key personnel have an open door to relate all security concerns upwards toward the executive suite. Gain the endorsement of the CEO in the importance of all cybersecurity investments and policies.

Assessment: Conduct a full cybersecurity risk assessment and present key findings to the CEO and Board. Put in place plans to lower risk consistently. Risk assessment would include: documenting assets and their reliance on technology, identify where threats exist in priority order and address them, buy cyber liability insurance, and put all needed protective measures in place, monitoring for updates as needed. Additionally, it's recommended that you have an outside expert run a penetration test on your network to identify any possible weaknesses.

Culture: Ensure cybersecurity is a consistent agenda item at management level. Put in place cybersecurity training as part of new staff onboarding and on an ongoing basis. Have all employees sign documents agreeing to adhere to all cybersecurity policies and procedures. Establish ongoing cybersecurity training and testing for all staff. Institute an annual review of the firm's cybersecurity posture and policies. Put in place multi-factor authentication (MFA) policies for any sharing or access to any level of company data.

(Continued on page 3)

Take Note

Security Video Podcast

Keep an eye out for details coming soon about an upcoming video podcast series on what your team members need to know about IT security.

March 31

World Backup Day

Avoid a potential disaster and back up your data files. Take the "World Backup Day Pledge" and sign up for a free backup review!

www.it-radix.com/review-my-backup

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

IT Radix Resource We make IT work for you

It's Time to Backup!

There is likely nothing more basic yet more important in information technology networks than a proper backup program being in place. Important data that is lost, stolen, or held for ransom can cripple an organization in an instant. That is why it is vital that managers ensure backups are in place and continually tested. You should be aware of your backup regimen.

Are you aware of the status of the "backup" of your data on your personal computer or on your organization's network or data in the cloud? In the IT world, folks talk of "backup and recovery" but what does that really mean. In short, backup is the system (usually automated software programs) that create and store copies of data. This provides protection from data being lost, stolen, corrupted or encrypted by bad actors. Recovery from a backup is the process of restoring original, unencrypted data to its original or alternate location.

Data Can Be Compromised in Many Ways.
This is important because data can be lost or ruined due to a variety of factors such as hardware or software failure, internal or external data corruption, malicious attacks via malware, viruses or social engineering and even accidental deletion of key data/information. In short, a backup allows data to be recovered and restored from an earlier point in time.

What Do IT Professionals Recommend for Backups?
IT professionals, such as the folks at IT Radix, typically recommend backups to be stored both locally (for ease/speed of recovery) as well as off-site (either in the cloud or in another location). If your data resides in the cloud, it's always wise to have a separate third-party backup in place for this data too. This ensures that whatever the cause for the data loss, a recovery can take place. They also advocate a retention plan that covers a wide range of data—more copies of more recent data, fewer of older data.

So, take this BEEP as a warning! Be sure your data on your computer is backed up and know what is being backed up and how frequently.

IT Radix Has You Covered.
You might decide that you need to take some action to get covered with a backup. IT Radix's managed service plans include a local and off-site backup that is proactively monitored and tested regularly. New to our managed services? You could win a fleece blanket and literally get yourself "covered" with a backup! As we like to say, when it relates to backup… "We've Got You Covered."

Learn more about how you too can be covered when it comes to IT backups and schedule a free consultation today!

Free Cybersecurity Audit Will Reveal Where Your Computer Network is Exposed and How to Protect Your Company Now

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 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**

Become a Smooth Operator

(Continued from page 1)

Software and Hardware Basics: Ensure the following are in place:

- **Schedule Ongoing Backups**. Having an up-to-date backup in place is the antidote for all these catastrophic events. A backup can be used to recover anything stored on the device in the event of an attack or other debacle.
- **Manage Access to Data**. Prevent access to your data from unauthorized individuals. Ensure that a strong, secure password policy is in place as well!
- **Ensure Endpoint Security**. All key hardware and software should be kept up to date by downloading software and firmware updates as they are deployed by each vendor. This is an often overlooked first line of defense for all networks. That includes having an anti-virus solution in place on all hardware and ensuring it is current.

Outside relationships: Evaluate all potential vendors considering their policies relating to the sharing of key organizational data. Evaluate potential strategic partners and potential acquisitions in the same vein.

Stay tuned next month as we shine a light on your internal IT Department and share what they need to know to keep your corporate data safe and secure.

"I think my spell-checker is broken. It keeps changing l-u-c-k to p-r-e-p-a-r-a-t-i-o-n."

Your Data is Out There

The hybrid work environment is here to stay. Work done away from a central office means data security is even more important. Here are a few "nevers" for hybrid work staff:

- Never log onto a free Wi-Fi network while working with confidential data.
- Never let anyone else use your corporate device. A child or spouse downloading malicious software to a corporate device can result in a ransomware attack or data breach.
- Never treat a corporate device casually. Whether it's a flash drive or a mobile phone, each can provide a way for criminals to access the network core.
- Never fail to report something that you feel might be a risk.

Data security is a big concern when you're away from the office. Stay safe and secure out there!

Welcome!

A warm welcome to our newest Management and Support clients:

Nest Global Solutions
Officemate
The Rippel Foundation

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

IT Radix Resource We make IT work for you

"Grow comfortable with risks, because adventures and unforeseen joys await those who say yes."

— Unknown

From the desk of Cathy Coloff

March Madness is upon us... as a Duke grad, it's fun to tune in to basketball games and relive my college days camping out to get a spot in Cameron Indoor Stadium to see Duke play UNC, our biggest rival. But March Madness is not just about basketball. It's about team performance. The teams have competed all year long to get to this point and have learned how to work together, adjusting along the way, to take advantage of each player's strengths.

Working together at IT Radix is similar—we all work together to serve our clients, helping their business succeed. Our team, like many, is composed of individuals with diverse backgrounds, skills, and education and we all enjoy helping others, solving problems, or finding solutions to meet our clients' goals. While there is no NCAA tournament for us to win, every time we receive positive feedback from our clients makes our team a champion in my eyes.

As for March Madness, go Duke!

security TIP of the month

Go Incognito!

Why? Web browser cookies are an essential part of the web. However, there are times where you want to protect your privacy and be more secure. If so, go incognito! Here's how:

Chrome, Edge, Safari:
Ctrl-Shift-N
(Command-Shift-N on Mac)

Firefox:
Ctrl-Shift-P
(Command-Shift-P on Mac)

Contact IT Radix for more tips on ensuring online privacy!

That's SOME PIG!

An interview with IT Account Services Coordinator, Amy:

IT Radix: How were you introduced to the idea of owning a pig?
Amy: When I was six years old, I saw the movie *Charlotte's Web*; and from that moment on, I knew I wanted a pig.

IT Radix: What do you like most about having a pig?
Amy: Having Ollie has helped me build awareness of the plight of pigs bred to be sold as pets. Ollie was a rescue. He was only three weeks old when I adopted him. He was living on a farm where the animals were being abused/neglected and was in dire need of a home. I had always wanted a pig, and it was even more special to be able to have the opportunity to rescue one.

IT Radix: How has having a pig enhanced your life?
Amy: Ollie is lovable, funny, and very entertaining! He brings me so much joy. Who knew pigs preferred to sleep *in* a mattress instead of *on* a mattress?

Ollie has become a "pig" part of Amy's life. Follow him and his latest shenanigans on Instagram: @olivermcwigglebottom

