TECH TIPS
TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON
CONSULTING & SOLUTIONS

Inside This Issue

February 2021

This monthly publication provided courtesy of Robert Zehnder President of Hodgson Consulting & Solutions.

Our Mission:

To eliminate every technical frustration, obstacle and inefficiency for companies with multiple locations and/or a remote workforce.

You NEVER See It Coming! But Once It Hits, Everyone Says, "I Wish I Would Have_____"

A year ago, no one could have predicted that countless businesses would shift to a remote work model. The pandemic hit hard and fast, and small businesses had to think on their toes. Many had only a few weeks to adapt. It was stressful and extremely challenging.

Looking back on it, many SMBs wish they'd had a plan in place that would have made things easier. When the pandemic hit in February/March 2020, SMBs had to absorb the huge cost of getting their employees up and running off-site. Not only was it costly, but it also took a lot of coordination and on-the-fly planning. This meant things slipped through the cracks, including cyber security.

As they say, hindsight is 20/20. You may wish you had a plan in place or had more time, but you didn't. A vast majority didn't. However, you can still plan for the future! While you never know when disaster is going to strike, you CAN be prepared for it. Whether that disaster is a pandemic, flood, fire or even hardware failure, there are steps you can implement today that will put you in a better place tomorrow. Here's how to get started.

Put Your Plan Into Writing.

First and foremost, you should have a standard operating procedure to call on should something go wrong. For example, in early 2020, many SMBs didn't have a security plan in place, let alone a *remote* work security plan. They had to make it up as they went, which just added to the challenges they were already experiencing.

To get over this challenge, work with an experienced IT services company or managed services provider (MSP) to put together a plan. This plan should include a cyber security

Continued on pg.2

Continued from pg.1

protocol. It should define what malware software employees should be using, what number they should call for 24/7 support, who to contact when they receive suspicious e-mails, how to identify suspicious e-mails and so on.

More than that, it should outline exactly what needs to happen when disaster strikes. Pandemic? Here's how we operate. Fire? Here's what you need to know. Hardware failure? Call this number immediately. The list goes on, and it can be pretty extensive. This, again, is why it's so important to work with an MSP. They've already put together plans for other SMBs, and they know where to start when they customize a plan with you.

Invest In Security And Backups.

While every business should have network security already in place, the reality is that many don't. There are a ton of reasons why (cost concerns, lack of time, lack of resources, etc.), but those reasons why aren't going to stop a cyber-attack. Hackers don't care that you didn't have time to put malware protection on your PCs; they just want money and to wreak havoc.

> **"When you have IT security in place, including firewall protection, malware software, strong passwords and a company-wide IT security policy, you put your business and all your employees in a much better place."**

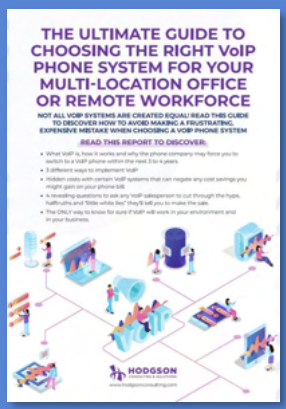
When you have IT security in place, including firewall protection, malware software, strong passwords and a company-wide IT security policy, you put your business and all your employees in a much better place. All of this should be in place for both on-site employees and remote workers. With more people working from home going into 2021, having reliable IT security in place is more important than ever before.

On top of that, you should have secure backups in place. Investing in cloud storage is a great way to go. That way, if anything happens on-site or to your primary data storage, you have backups you can rely on to restore lost or inaccessible data. Plus, having a solid cloud storage option gives remote employees ready access to any data they might need while at home or on the go.

Where Do You Begin?

Some SMBs have the time, money and resources to invest in on-site IT personnel, but most don't. It is a big investment. This is where partnering with an experienced IT services firm can really pay off. You may have employees in-office or you may have a team working remotely – or you may have a mix of both. You need support that can take care of everyone in your organization while taking care of the data security of the business itself. This is where your IT partner comes into play. They are someone you can rely on 24/7 and someone who will be there for you during a pandemic or any other disaster.

FREE Report: "The Ultimate Guide To Choosing The RIGHT VoIP Phone System For Your Small Business, Call Center Or Multi-Location Office"

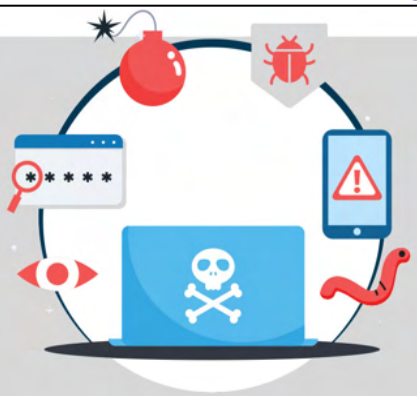


You'll Learn:

- What VoIP is, how it works and why the phone company may force you to switch to a VoIP within the next 3-4 years.
- 3 different ways to implement VoIP.
- Hidden costs of certain VoIP systems that can negate any cost-savings you might gain on your phone bill.
- 4 revealing questions to ask any VoIP salesperson to cut through the hype, half-truths, and "little white lies" they'll tell you to make a sale.
- The ONLY way to know for sure if VoIP will work in your environment and in your business.

Get your FREE copy today at:
www.hodgsonconsulting.com/7voipquestions/

DETECT VULNERABILITIES WITH REGULAR RISK ASSESSMENTS



$3.86M

The average cost of a data breach is **$3.86 million**, which should give you an idea of what is at stake.[2] Without risk assessments, you have no other way of analyzing vulnerabilities in your networks and applications.

By performing an IT security risk assessment, not only can you identify hard-to-detect issues and come up with the necessary fixes, you can also devise an action plan to track the progress of your remediation.

You can also get a better understanding of your risks with a risk-scoring algorithm. Here, the risk scores assigned to various threats based on their impact can help you prioritize your fixes and get a better measure of your network.

BENEFITS OF IT SECURITY RISK ASSESSMENT

By performing regular network risk assessments, you can:

- ✔ Gain detailed visibility into an IT network to analyze all security threats and undetected issues
- ✔ Develop solutions based on the issues detected by the assessment and protect your IT infrastructure from various external and internal threats
- ✔ Prioritize remediation of various issues and measure overall network health
- ✔ Protect your assets and guard against unexpected downtime
- ✔ Detect anomalous activities by methodically analyzing your login history

Sources

[1,2] Cost of a Data Breach Report 2020 - IBM

WHY YOU NEED A TRUSTED PARTNER

Having a trusted MSP partner to navigate through the complexities of IT security risk assessments can help you focus on other productive tasks and bring you much-needed peace of mind.

With years of expertise in IT security, we can take care of your risk assessments and eliminate any hassles you may face in the process. **With our expertise, you can:**

- Easily identify vulnerabilities in your network
- Develop an action plan to boost IT security
- Measure your overall network health
- Make informed decisions on IT security measures

Call Now to Schedule Your IT Security Risk Assessment Today!

3 Ways To Protect Your Data During COVID-19

1. Manage Your Passwords. *You've* heard it before, and you'll hear it again – one of the best ways to keep intruders out of your data is to lock it behind strong passwords that are updated every 60 to 90 days. Use passwords that are a mix of letters, numbers and special characters. Make passwords long and confusing.

2. Secure All Data. Who are you sharing your data with? Do former employees still have access? What about former clients? Take time to see who has permission to access your network and data. While you're at it, clean up old or useless data that may be just taking up space. When you know what data you're saving – and who has permission to access that data – you can better protect it.

3. Adopt Best Practices. When was the last time your team received IT security training? Never? Five years ago? It's time to get back on it. Train your team on the latest cyber security threats and how to handle them. Then, adopt best practices so your team knows what to do when they receive a phishing e-mail or there's a threat to your network. *Inc., Nov. 20, 2020*

Confidence Is Key: How To Self-Promote For Greater Success

We often don't like to talk about ourselves. But there are many times when it is important to talk about yourself and to convey your accomplishments. Maybe you're applying for a new position within your organization, you're trying to establish a partnership with another company or you want to expand your professional network. Either way, here are a few ways to self-promote without sounding like a brag.

Lean Into Your Expertise. Call on your experience. If someone is dealing with an issue you're familiar with, walk them through it. Or, take on the role of mentor with others in your organization or community.

Be Receptive To Feedback. This is how we grow. Listen to what people have to say and respond by taking action. Make adjustments as they make sense. When you receive positive feedback, accept it graciously.

Emphasize "Together." Don't make things just about you. Share credit when it deserves to be shared. Be a supportive and motivational voice. Uplift others. *Forbes, Nov. 23, 2020*