TECH TIPS

TECHNOLOGY INSIGHT THAT BUILDS BUSINESS

HODGSON
CONSULTING & SOLUTIONS

Inside This Issue

May 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.

How To Make Cyber Security An Ingrained Part Of Your Company Culture

Your employees are your first line of defense when it comes to protecting your business from cyberthreats. Human error is one of the single biggest culprits behind cyber-attacks. It comes down to someone falling for a phishing scam, clicking an unknown link or downloading a file without realizing that it's malicious.

Because your team is so critical to protecting your business from cyberthreats, it's just as critical to keep your team informed and on top of today's dangers. One way to do that is to weave cyber security into your existing company culture.

How Do You Do That?

For many employees, cyber security is rarely an engaging topic. In truth, it can be dry at times, especially for people outside of the cyber security industry, but it can boil down to presentation. That isn't to say you need to make cyber security "fun," but make it interesting or engaging. It should be accessible and a normal part of the workday.

Bring It Home For Your Team. One of the reasons why people are often disconnected from topics related to cyber security is simply because they don't have firsthand experience with it. This is also one reason why many small businesses don't invest in cyber security in the first place – it hasn't happened to them, so they don't think it will. Following that logic, why invest in it at all?

The thing is that it will eventually happen. It's never a question of if, but when. Cyberthreats are more common than ever. Of course, this also means it's easier to find examples you can share with your team. Many major companies have been attacked. Millions of people have had their personal data stolen. Look for examples that employees can relate to, names they are

Continued on pg.2

Continued from pg.1

familiar with, and discuss the damage that's been done.

If possible, bring in personal examples. Maybe you or someone you know has been the victim of a cyber-attack, such as ransomware or a data breach. The closer you can bring it home to your employees, the more they can relate, which means they're listening.

Collaborate With Your Employees. Ask what your team needs from you in terms of cyber security. Maybe they have zero knowledge about data security and they could benefit from training. Or maybe they need access to better tools and resources. Make it a regular conversation with employees and respond to their concerns.

Part of that can include transparency with employees. If Julie in accounting received a phishing e-mail, talk about it. Bring it up in the next weekly huddle or all-company meeting. Talk about what was in the e-mail and point out its identifying features. Do this every time phishing e-mails reach your employees.

Or, maybe Jared received a mysterious e-mail and made the mistake of clicking the link within that e-mail. Talk about that with everyone, as well. It's not about calling out Jared. It's about having a conversation and not placing blame. The focus should be on educating and filling in the gaps. Keep the conversation going and make it a normal part of your company's routine. The more you talk about it and the more open you are, the more it becomes a part of the company culture.

> **"For the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture."**

Keep Things Positive. Coming from that last point, you want employees to feel safe in bringing their concerns to their supervisors or managers. While there are many cyberthreats that can do serious damage to your business (and this should be stressed to employees), you want to create an environment where employees are willing to ask for help and are encouraged to learn more about these issues.

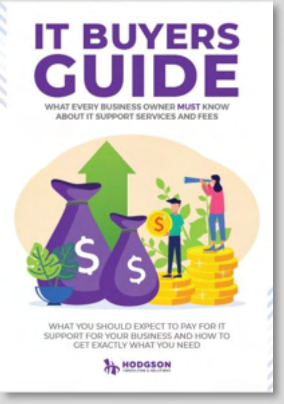
Basically, employees should know they won't get into trouble if something happens. Now, if an employee is blatantly not following your company's IT rules, that's a different matter. But for the day-to-day activities, creating a positive, educational, collaborative environment is the best way to make cyber security a normal part of your company culture.

Plus, taking this approach builds trust, and when you and your team have that trust, it becomes easier to tackle issues of data and network security – and to have necessary conversations.

Need help creating a cyber security company culture that's positive? Don't hesitate to reach out to your managed services provider or IT partner! They can help you lay the foundation for educating your team and ensure that everyone is on the same page when it comes to today's constant cyberthreats.

Free Report: IT Buyers Guide

What Every Business Owner MUST Know About IT Support Services And Fees


IT BUYERS GUIDE
WHAT EVERY BUSINESS OWNER MUST KNOW ABOUT IT SUPPORT SERVICES AND FEES
WHAT YOU SHOULD EXPECT TO PAY FOR IT SUPPORT FOR YOUR BUSINESS AND HOW TO GET EXACTLY WHAT YOU NEED
HODGSON

You'll learn:

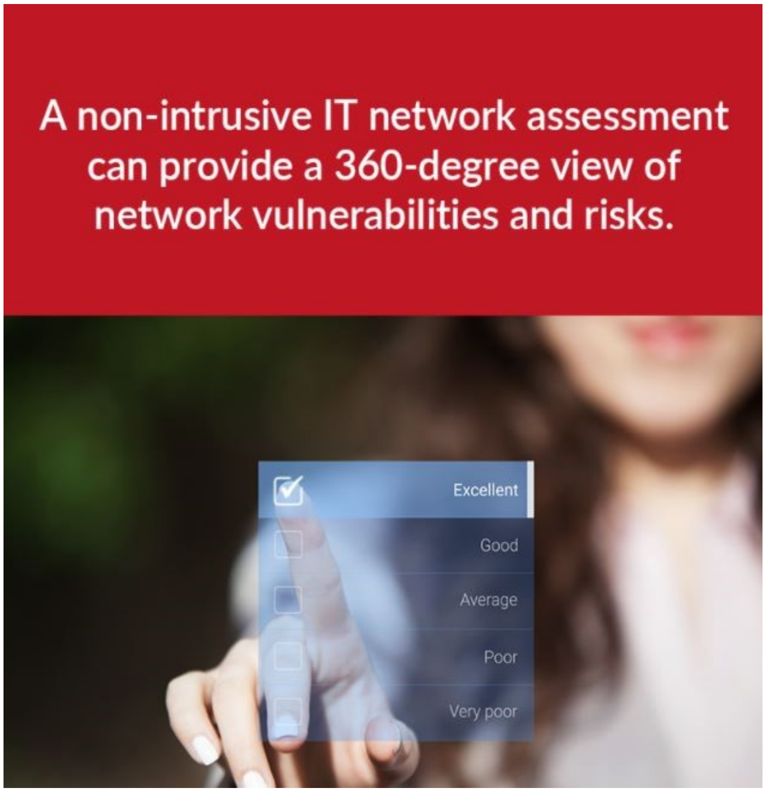
- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate

Claim your FREE copy today at www.hodgsonconsulting.com/IT.buyers.guide

Do You Know The Current Health Of Your IT Network And Business Solutions?

The cost of insider threats rose to **$11.45 million** in 2020.

Ponemon



A non-intrusive IT network assessment can provide a 360-degree view of network vulnerabilities and risks.

Less than 46% of organizations have evaluated their business continuity risks concerning cloud solutions.

Data Health Check 2020 Report

■ How To Know It's Time To Start Scaling Your Business

Creating a business that is scalable isn't easy, but it's necessary if you intend to grow – and grow some more. There are three simple ways to tell if you've created a business that is scalable.

You Have Positive Cash Flow Figured Out. You've successfully built a reliable month-to-month revenue stream. It's money that you can use to invest further into your business – whether it's to pay for additional employees, technology, systems and processes or all of the above.

Everything Has Been Delegated. Delegating is hard for many entrepreneurs. You want to have a hand in everything. But when your team keeps everything running – and everything runs even when you're not there – you're in a great place to scale up.

You Have More Control Over The People You Get To Work With. Basically, you can start to shape your client base. If there is someone you want to say no to (say you don't have the full resources to fulfill their needs or they're just not a great fit), you can move on guilt-free.

If you have these three things in place, you have the foundation to scale up safely and to create the business you've always wanted. *Forbes, Feb. 11, 2021*

■ How To Build A Forward-Thinking Customer Culture In Your Small Business

How well do you know your customers and clients? If you want to deliver a stellar customer experience and have a forward-thinking customer culture within your organization, you need to know your customers. What makes them tick? What do they love? Why do they make the decisions they make?

More than that, you need to go after the customers who make the most sense to your business. As you grow, you have more opportunity to be picky, so be picky! Develop the customer base you really want. That makes it easier to market to them, because you're all on the same page.

Finally, when you know who you want to target, stay consistent in your messaging. The entire customer experience – from online marketing to your storefront – should all be uniform. Consistency helps build your brand and anchors customers to the overall experience. *Forbes, Feb. 15, 2021*

MICROSOFT: Ending Open Licensing

So what does that mean?

Microsoft recently announced some changes that will take place early next year regarding the current structure of their licensing program. Naturally, you're probably wondering a few things 1.) What are the changes? 2.) How do they affect you?

Currently, Microsoft operates under their Microsoft Open License program, which was created over 20 years ago. This program was designed with small and mid-sized companies in mind, as described by Microsoft. The program was structured to help those parties who essentially needed to buy multiple licenses at volume prices.[1]

So what are the changes?

Effective January 1, 2022, customers will no longer be able to purchase new or renew existing licenses through Microsoft's Open License program. Instead, Microsoft will be transitioning to what they are calling their Open Value Subscription program.

The Microsoft Open Value Subscription program means that customers will now need to interact more with their Microsoft partners in the Cloud Solution Provider program and make their subscription purchases through them.

What do you need to know going forward?

"Microsoft Cloud Solution Provider (CSP) partners will be the partners that will offer perpetual licenses after the end of the Open License program. Perpetual licenses are pay-once, non-subscription licenses that don't expire. If organizations are using Software Assurance (SA) with those perpetual licenses, which lets them migrate to the latest software release, then they'll only be able to buy SA through a program different from the Open License program in 2022."[2]

As a Microsoft partner, Hodgson Consulting & Solutions will continue to keep you updated as the details of these changes continue to unfold.

[1] https://www.microsoft.com/en-us/licensing/news/microsoft-open-license-program-changes

[2] https://redmondmag.com/articles/2020/10/01/microsoft-ending-open-license-program.aspx