MAY 2021

InTech Intelligencer

"Insider Tips To Make Your Business Run Faster, Easier And More Profitably"

"As a business owner, you don't have time to waste on technical and issues. That's where we *shine*! Call us and put an end to your IT problems finally and forever!"

- Leia Shilobod,
President & I.T. Princess of Power

Inside This Issue…

InTech SOLUTIONS

One Northgate Sq., Ste. 202
Greensburg, PA 15601
724.235.8750

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 familiar with, and discuss

Continued on pg.2

Continued from pg.1

the damage that's been done.

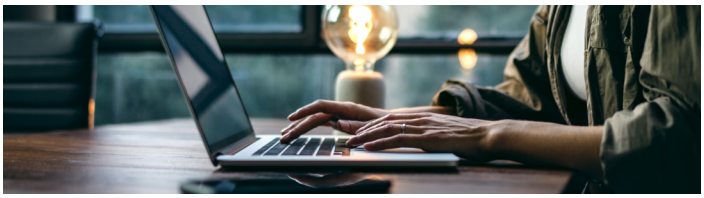
If possible, bring in personal examples. Maybe you or someone you know has been the victim of a cyber-attack, such as ransomware or a data breach. The closer you can bring it home to your employees, the more they can relate, which means they're listening.

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.

Call today to schedule a Cyber Security Risk Assessment for your business. 724.235.8750 or email Leia@intechit.net.

Free Report Download:
Questions You Should Ask Any IT "Expert" Before Letting Them Touch Your Network

How can you tell if you are going to receive poor or substandard service? How do you know if your computer guy or network consultant is doing everything possible to secure your network from downtime, viruses, data loss or other frustrating and expensive disasters? Could your current provider actually be jeopardizing your network?

This valuable Free Report helps you avoid common pitfalls of choosing an IT provider. Download yours today!

Claim Your FREE Copy Today at www.intechit.net/whattoask

Shiny New Gadget Of The Month:

The Pocket Translator: MUAMA ENENCE

It used to be science fiction, but not anymore! Now, you can translate languages on the go! The Muama Enence is the device that makes it possible. This handheld "listener" is capable of real-time translation of over 36 common languages from around the globe. Smaller than a smartphone, the Muama Enence breaks language barriers and makes travel easier than ever before, whether you're traveling for business or for vacation.

The Muama Enence is super-easy to use and ultra-portable. All you need to do is press a button, and it does the rest. Plus, with excellent audio quality, you'll be able to hear the translation, even when things get busy around you. Learn more – and get your own – at bit.ly/37hhn8R.

Lead Like Your Life Depends On It

Great leaders are like drug addicts. Here's what I mean by that: in my journey from being a homeless drug addict with no college degree to becoming a successful leader, I have learned that the leaders who are supposedly great, today and of the past, look like addicts in active addiction – they are fixing, managing and controlling perception to get what they want.

I look at the great leaders emerging today, and those who will surface tomorrow, and I see people who will lead in a fundamentally different way – they will look like addicts in recovery. But there's more to it than that. Consider the following questions:

- In the last 30 days, have you said yes to something you could say no to?
- In the last 30 days, have you hit a weakness?
- In the last 30 days, have you avoided a difficult conversation?
- In the last 30 days, have you held back your unique perspective?

As leaders, we perform these "actions" all the time. I call them our "masks" because we're hiding our true selves behind our actions.

Leaders teach others that they need to hide their vulnerabilities, imperfections or weaknesses in order to be successful. To put on a mask. I want to talk about taking off the mask (pandemic aside!), but this isn't about any physical mask. It starts by identifying what mask is holding you back. These are the four masks:

1. **Saying Yes When You Could Say No**
2. **Hiding A Weakness**
3. **Avoiding Difficult Conversations**
4. **Holding Back Your Unique Perspective (You Don't Speak Up When You Could/ Should)**

You can learn more about the mask that's holding you back at MaskFreeProgram.com. This is a free, five-minute assessment that will give you a clearer picture about which mask is holding you back. But more than that, it also gives you an authenticity rating – to help you determine how authentic you are.

What does authenticity have to do with masks? When you're wearing a mask, you are not being authentic – your true self. This rating tells you how close you are to being your true self.

So, how do you remove the mask? How do you become more authentic? Mask recovery comes down to three principles:

1. **Practice Rigorous Authenticity** — Be true to yourself all the time, no matter the cost.
2. **Surrender The Outcome** — Leaders are taught to obsess over outcomes; focus on what you can control.
3. **Do Uncomfortable Work** — With this emotional work, we need to take action that is good for us (saying no, having difficult conversations).

When you focus on these three principles, you become more authentic. You are able to grow and become the leader for the future – like an addict in recovery.

Michael Brody-Waite is a recovered drug addict who has since become a three-time CEO and TEDx speaker (with over 1.5 million views). He's held a leadership role at a Fortune 50 company, he's the founder of an Inc. 500 company, he's led a nonprofit and he's the author of Lead Like Your Life Depends On It: Why In A Pandemic Great Leaders Lead Like Drug Addicts.

Need NIST 800-171 | CMMC Compliance?

For businesses in the DoD Supply Chain who need to comply with NIST 800-171 Security Protocols and CMMC, InTech provides Risk Assessments, Security Audits, Compliance Audits, Plans of Action, and Remediation to bring YOU into compliance and assure you keep your contracts. Start the process today with a free, no obligation survey to get an idea of what you need to do to come into compliance. Go to **www.intechit.net/NISTassessment** and take just 5 minutes to jump start compliance.

Who Else Wants To Win A $25 Gift Card?

You can be the Grand Prize Winner of this month's Trivia Challenge Quiz! Just be the first person to correctly answer this month's trivia question and receive a $25 Visa gift card Ready?

Google's first tweet on Twitter was a message encoded in binary that read what?

a. Don't be evil
b. I'm feeling lucky
c. Do the right thing
d. Is this thing on?

Email us right now with your answer!
info@intechit.net

One Northgate Sq., Ste. 202
Greensburg, PA 15601

US POSTAGE
PAID
GREENSBURG, PA
PERMIT NO. 1117

- RETURN SERVICE REQUESTED—

"NIST 800-171 and CMMC – Your Most Asked Questions "

InTech has been serving companies in the DoD Supply chain since 2006, and helping companies get compliant with NIST 800-171 and CMMC since 2017. While there is so much to discuss about compliance, here are the questions we get asked the most:

What is CMMC? The Cyber Security Maturity Model Certification is a process of certifying companies at one of 5 security levels who contract with the federal government or are at some layer of the supply chain.

How is CMMC related to NIST SP 800-171? NIST Special Publication 800-171: Securing Controlled Unclassified Information on Non-Governmental Systems was authored by the National Institute of Standards and Technology as standard controls for IT and Physical Security Systems when there is CUI on those systems. If you handle CUI, you'll need to certify at Level 3 or above for CMMC.

I have until 2025 to certify, right? Kind of. All 300,000 companies in the supply chain will need to be certified by 2025, so its very likely you'll need to certify way before 2025. We recommend you're ready in the next 12-18 months to be safe. There is usually a lot to do, and an investment to make.

What are the biggest ways companies fail CMMC? The biggest gap we see is lack of the required documented Policies, Plans, and Procedures. Every single company we have worked with has this gap. Aside from documentation, having a clear understanding of what your company has custody of that is CUI, and the approved methods for CUI in flow, internal handling, and outflow is unclear or completely missing.

Is CMMC | NIST 800-171 Compliance expensive? That depends. You can be certain you will have an investment of time, and its likely you'll need to make some technology changes or additions. Its also possible you'll need to change some business processes, which may or may not have a financial impact.

Can I do this on my own? Yes you can. But even seasoned IT professionals ask me what some of the controls actually mean, so becoming a part of the larger community for support and information is vital. If you choose to engage with a partner or consultant for help, be sure you understand the deliverables and that you will receive a clear roadmap for compliance.

This seems like so much work and cost. Why are they doing this? While it can sometimes feel like an unnecessary burden, remember this is for a purpose. Our country loses billions of dollars a year to malicious actors and our defense information to foreign governments positioned as a threat to us. It is our duty to secure our company by means of the sensitive information entrusted to us.

To Your Success,