JULY 2022

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

Do I Need A Compliance And Cyber Security Plan?

We talk a lot about cyber security and how incorporating the right practices can help fully protect your company from cyber-attacks, but there's another term that's often referenced when discussing cyber security that's just as important: compliance. While it's incredibly important for businesses to focus on maintaining the highest cyber security standards, they also need to ensure protocol meets compliance standards.

In regard to cyber security, compliance typically relates to processes and controls that help protect the confidentiality and accessibility of certain information for how its stored, processed or transferred. There is no overarching standard for compliance. Instead, you'll find different guidelines and requirements for different industries, or for the type of data/information concerned. It's important to be aware of your company's specific requirements. If you're not, you could be subject to fines and penalties in addition to being at greater risk for cyber-attacks.

Though they're related, there are still some glaring differences between cyber security and compliance. Cyber security is practiced for the company's own sake instead of to satisfy the needs of a third party. It's also present to protect a business from the risk of constant threats and needs to be continually managed and updated. IT compliance, however, is completed to satisfy external requirements. Unlike cyber security, compliance is finished when the third party is satisfied with the alignment to controls or standards.

Compliance and cyber security work best when they're aligned, so it's extremely important that your business has IT Security Policies in place that guide the organization's decisions. Your Policies are like your bible, and change rarely, but must be approved by leadership and lived throughout the organization.

Policies should be aligned with compliance requirements, because failure to comply can carry huge fines or loss of contracts/business.

Continued on pg.2

Continued from pg.1

Then you need to create plans which operationally assure continuous alignment to those standards and requirements, as well as monitoring and assessment of networks, devices and systems that your company uses in order to align with regulatory cyber security requirements. This allows you to set up an action plan for realignment.

Plans, such as Incident Response Plans (IRP), are also vital if your business is ever breached as you need to communicate news of the breach to any parties that could've been impacted or regulatory authorities.

Every business, regardless of size, is susceptible to data breaches and attacks by malicious actors. It's only with strong cyber security and IT plans in place that you can have a high level of confidence that you've done due diligence to plug the holes hackers look to exploit.

Plans to assure continued alignment are a great start, but having the right cybersecurity measures in place will are prepared if you're ever audited by a third party.

"Compliance and cyber security work best when they're aligned, so it's incredibly important that your business has a plan for compliance and cyber security."

Once Policies and Plans are implemented, you can focus on accurately documenting the day to day processes your company need to take to stay secure and compliant in the areas of IT, personnel, and physical security. Cybersecurity and compliance is no longer the wild west. Everything must be documented. From agendas, to meeting notes, to the changes to the IT systems, documentation of requests to access data, to new users added to the system, to the list of items that an auditor may need, your entire team needs to document anything they do or see regarding cyber security or that can impact compliance.

We started working with companies in the Department of Defense's Supply Chain (DiB) years ago and ran up against the need for compliance to the NIST 800-171 controls, which have parlayed into CMMC today. We thought it would be easy to do an IT project to align the company we would be compliant. We found out that just didn't work. Compliance is not just an IT function, and STAYING compliant was challenging.

That's when we created a Proven Process to get and keep our clients compliant. We start with understanding the data you need to protect and how its handled and aligned with business processes, then assess gaps in compliance and create a discrete plan to get aligned with compliance.

With a list of projects and their associated costs, our clients have a Roadmap to get compliant, then we keep them compliant overtime through Risk Assessments and Management.

If your company faces compliance requirements or is having concerns with cyber insurance questionnaires, you can hop on the line with me for a quick chat to answer burning questions and see if we can help. Just call 724.235.8750 or email Leia@intechit.net and ask for a Risk Assessment Call.

To your security,
Leia Shilobod, CISM
CEO, InTech Solutions, Inc.

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:

Airmoto

Imagine you're driving with your family on vacation in the middle of winter. All of a sudden, the road feels much bumpier, so you pull over and get out to check your tires. To your dismay, you discover one of your tires has gone flat. The closest gas station is over a couple of miles away, and your spare can't handle the adverse conditions. So, what should you do? With Airmoto, you never have to worry about this situation.

Airmoto is a rechargeable compact air pump that provides up to 120 psi. In only 10 minutes, you can inflate your car's tires to the proper tire pressure. Airmoto can be used to pump up balls, bike tires and even truck tires. It's practical, not very heavy and quite affordable. Airmoto is the perfect addition to any roadside assistance kit.

8 Tips To Reach The Top Of Your Field

I've been consulting business leaders for well over 20 years now, and in that time, I've worked with some of the brightest minds across various industries. At ghSMART, we have helped many people reach the top of their field, and you may be wondering how we helped them. A professor taught me a tactic years ago that has helped me reach the top of my field. Now, I enjoy sharing this information with our clients.

Essentially, there are three roles in every profession – rainmakers, doers and trackers. The trackers are those who track other people's work. They play an important role but will rarely leave a lasting impact on their field.
Most people are doers, since they do the work that is provided to them by someone else. They're also important, but they probably won't reach the top of the field. Then there are the rainmakers. These are the people who are proactive and go above and beyond to achieve results. Rainmakers always push to reach their goals and often reach the top of their field in the process.

Just being a rainmaker is not enough to leave an impact, though. If you follow these eight tips, you'll be well on your way toward success.

- Go to the best schools you can while achieving the highest grades possible and establish your technical skills. You don't necessarily have to attend the best school possible, but it does help.
- Spend 20% of your time building relationships. Try to spend a day each week learning what concerns are affecting customers in your industry and work toward solutions.

- Keep a list of your 50 most important relationships and rank them in order of importance.
- Don't do tasks or offer advice if it is outside of your area of expertise. If you don't deliver great results, you will push your clientele away.
- Improve your public speaking skills. On average, 95% of professionals are not confident when speaking in public, so the 5% who are confident usually shine on a regular basis.
- Learn how to hire and delegate. You can't do everything on your own, so you need to surround yourself with a team you can trust.
- Price yourself high, but don't get greedy. You know how much your work is worth and you know how much the competition charges. For desired results, clients don't mind paying a little extra for good work.
- Mentor others to become rainmakers. Your team will only grow stronger.

As a caring and courageous rainmaker, you will rise to the top of your field – while your peers who rest entirely on their technical skills will not.

Dr. Geoff Smart is the chairman and founder of ghSMART, a leadership consulting firm that exists to help leaders amplify their positive impact on the world. Dr. Smart and his firm have published multiple New York Times best sellers. He stays active in his community and has advised many government officials.

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?

Where is Microsoft's headquarters?

a) Silicon Valley, CA
b) Redmond, WA
c) Tampa, FL
d) Los Angeles, CA

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

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

"Do I Really Need Cyber Insurance?"

Short Answer: YES.

Longer Answer: Clients, prospects, and other IT Providers ask me this on the regular. In fact, in June, I was asked to speak to 3,000 IT Providers and internal IT about this very thing.

Insurance does not protect you from major incidents, it transfers risk related to ransomware incidents. This means you need to assess the risk cyber incidents may pose to your business and implement strategies to mitigate that risk.

What does that look like? If you're an InTech client, we're having Strategic IT or Risk Management Meetings with you were we are assessing the risks together and bringing forward potential solutions to mitigate the risks.

If your IT provider doesn't do this with you, the insurance questionnaire is a great mechanism to get your organization talking about the risks – and what changes you should make to mitigate them.

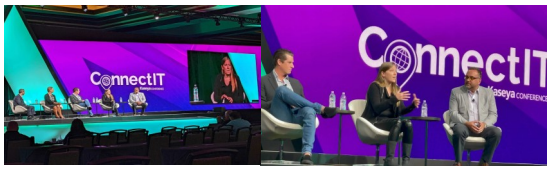
Every business will have an Incident, so you need to assure you've got an Incident Response Plan (IRP). You should also be performing tabletop exercises (a walkthrough of how you respond to an incident) AT LEAST once a year.

You also need to thoroughly understand your cyber insurance policy requirements for what actions you need to take when you have an incident. If your MSP responds and that response is not in line with your policy requirements, they could void the ability for your claim to be paid.

And please, please, please, DO NOT simply hand your insurance questionnaire to your IT Provider and expect them to answer it without you. You must understand the questions and answers. This is YOUR application and you're signing it, so it's your risk.

To Your Success,

Leia



Leia Shilobod, CISM | CEO | Cybersecurity SME speaking at Kaseya ConnectIT to over 3000 MSPs about Cyber Insurance