THE PROBLEM SOLVER

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

What's New

Security Regulations are Evolving!

Join us on September 30th at 11AM for our live webinar:

The Evolution of Security Regulations in 2020.

We'll be taking a look at security, risk and compliance issues that should be re-evaluated, especially if your working environment has changed.

Sign Up Today!

September 2020

This monthly publication provided courtesy of Karyn Schell, President at DP Solutions.

Our Mission: To build a community of successful-minded entrepreneurs that inspires excellence, encourages collaboration and expands the capacity of all members to achieve great things.

Sneaky Ways Cybercriminals Attack Your Network

And What You Can Do To Prevent It NOW

If you own a small business, your business is a target for hackers. According to a report by 4iQ, a cyber security analyst firm, from 2017 to 2019, there was a 424% increase in the number of attacks on small businesses.

At the same time, a survey by The Manifest, a business analyst firm, found that 64% of small businesses intended to put more time and money into their IT security in 2020. Many business owners also noted an increase in attacks against their businesses and websites and were ready to do more to protect themselves.

Cybercriminals love to go after small businesses. Since small businesses make up 99.7% of all employers in the United States, you can see why it makes sense. Hackers know that attacking small businesses can be worth the time and effort because they know they will eventually find a small business they can extort or steal from.

It all comes down to cyber security. If you have inferior network security (or none at all), you're a prize for hackers. They have all kinds of tools at their disposal to get what they want. If you're not careful, and if you haven't invested in good network security, you may quickly find yourself becoming a victim of those tools.

Some of the hacker tools are much sneakier than many people realize. Here are two major examples.

Phishing Scams

Hackers know one of the easiest ways to break into a network is to bypass practical security altogether. Instead, they go after the human element. They send e-mails to unsuspecting recipients

Continued on pg.2

Continued from pg.1

in the hope that those recipients will open the e-mail and follow the false instructions.

The criminal may include an attachment. When clicked, the attachment installs malware on the victim's computer. The malware might look for private information, like financial numbers or personal information, or it may lock the computer down until the victim pays an exorbitant sum.

The criminal may include a link to another website. Phishing e-mails can look like legitimate messages from well-known companies, such as Chase, PayPal or Amazon. These e-mails often tell you that your account has been compromised, a phrase that is designed to scare victims into clicking the link and providing their personal information to protect the account. Put that information in, and you hand over that information to the criminal. This is why employee cyber security training is a must!

Password Exploits

Many people don't realize how dangerous it is to reuse the same username and/or password for everything – or to never update their passwords. It's very likely that at least one of your active passwords has fallen into the hands of hackers. They may have gotten it years ago from a website that doesn't exist anymore. But if you are still using that same username and password for other websites and accounts, you are putting yourself at risk.

"According to a report by 4iQ, a cyber security analyst firm, from 2017 to 2019, there was a 424% increase in the number of attacks on small businesses."

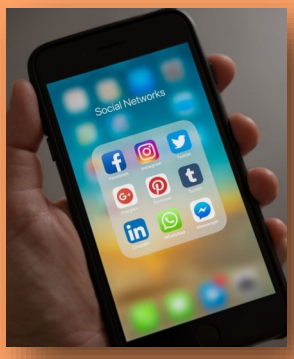
According to Trace Security, nearly 80% of all data breaches are the result of simple or reused passwords. Some of the most popular passwords today include things like "12345," "password" and "qwerty." Even worse, many businesses use passwords like these to protect sensitive data such as banking information and customer records. If a password is old or easily guessed, it offers nearly the same protection as no password at all! Change your passwords at least every 60-90 days and use different but secure passwords for everything.

The great news is that it's easier than ever to protect your business from things like phishing scams, data breaches and so much more. Just because you haven't had any major problems for years, or at all, doesn't mean you should assume nothing will happen in the future. You might also think that you simply don't have the time or resources for good security.

The even better news is that you don't need to spend a lot of time or money to secure your business against hackers and cybercriminals. All you really need to do is partner with an IT services firm that knows cyber security inside out.

When you work with a dedicated IT security company, they take care of you. They can monitor your network 24/7 and make sure the bad guys don't get in. They can make sure your data is backed up to a secured server so that if anything does go wrong, you don't lose a beat. They can even provide you with round-the-clock support should you have any questions or concerns. It's a surprisingly easy and cost-effective way to protect your business and to put the cybercriminals in their place.

Social Media Threats in 2020 (Video Blog)



Between Facebook, LinkedIn, Twitter, Tik Tok, Instagram, and whatever other Social Media platforms that are on the horizon, our lives are more public than ever before. There are definitely upsides and downsides to this landscape, but I'm not here to talk about that today. Whether we like it or not, it's clear that Social Media is here to stay.

In this video Ben will talk about is what we should be thinking about as we engage with these platforms. What can we do as individuals to limit the downsides and risks associated with having a social media presence? Let's take a moment to go over a few important tips to keep in mind in 2020.

Learn about these important tips here:
https://www.dpsolutions.com/blog/social-media-threats-2020

Tech Tip

"Is the router your ISP gave you safe?"

Your WiFi router could be posing a security risk. Here's what you need to know.

When most people subscribe to an Internet Service Provider (ISP), they get a little router and some simple instructions on how to get started. They may hook up a WiFi Access Point, but then the device sits in the corner only to be touched when the connection fails, and they perform the ubiquitous power cycle.

As long as there aren't any problems, these devices typically stay untouched until the device stops working entirely, and a new one is sent. But if that doesn't happen, the device just sits indefinitely. Is that a problem? Yes!

We all know that every so often we'll hear from our IT person that it's time to upgrade Windows or another application, because they system is no longer supported by the vendor.

So if your home router hasn't been replaced in years, it might be time to reach out to your ISP and ask about your options, or what they are doing to make sure this device is secure. While most routers are fairly safe, you want to make sure you take potentially risky devices out of production.

Building Your Legacy – Yes, Even Now

When it comes to your business, what does creating a legacy mean to you?

When I was interviewing business leaders and owners for *Fix This Next*, I made a profound discovery. The ones who had already achieved the first four levels of my Business Hierarchy Of Needs and were in the Legacy level said they are not business owners.

You know what they told me? They are business stewards. They never really "owned" their businesses. Their job was to raise their business to be independent of them. Eureka! What a profound realization.

As a steward of your business, it is your responsibility to bring life to the business. More importantly, it is about that business continuing to prosper without you! To create a legacy, you must create permanence in your business. It must be designed to run on its own.

Legacy is not about money, power or how much fame you have. As a young entrepreneur, that's sure what I thought it was about. Legacy is all about your business continuing to impact your community, your customers, your culture and the world – without your participation.

Apple runs without Steve Jobs. Mary Kay runs without Mary Kay. Countless companies are living long after the involvement of the business owners ended. And that is exactly what the founders wanted.

We've been looking at The Business Hierarchy Of Needs, and Legacy is way up at the top. To achieve the Legacy level, the owner must care more about the corporate legacy than their personal legacy. This should be the objective of your business.

So what is the recipe to leave your legacy? Let's get into the 5 Vital Needs of the Legacy level.

1. Community Continuance – Do your clients support your business? Do they support it in a way that is authentic to your intentions?

2. Intentional Leadership Turn – Is there a plan for leadership to transition and stay fresh? Do you have a plan for people to take over leadership of your business when you are ready to move on?

3. Heart-Based Promoters – Is the organization promoted by individuals inside and outside of it, without the need for direction? Do they see the greater mission and become curators themselves?

4. Quarterly Dynamics – Does your business have a clear vision for the future? Does it dynamically adjust quarterly to make that vision a reality?

5. Ongoing Adaptation – Is your business designed to constantly adapt and improve? Does it find ways to get better and beat itself?

Review these 5 Vital Needs within your business and assess where you are in leaving your own legacy.

Legacy isn't about going public or making billions of dollars. Legacy is about making your mark on the world the way you intended.

MIKE MICHALOWICZ (pronounced mi-KAL-o-wits) started his first business at the age of 24, moving his young family to the only safe place he could afford – a retirement building. With no experience, no contacts and no savings, he systematically bootstrapped a multimillion-dollar business. Then he did it again. And again. Now he is doing it for other entrepreneurs. Mike is the CEO of Provendus Group. He is also a former small-business columnist for The Wall Street Journal*; MSNBC's business makeover expert; a keynote speaker on entrepreneurship; and the author of the cult classic book* The Toilet Paper Entrepreneur. *His newest book,* The Pumpkin Plan, *has already been called "the next E-Myth!" For more information, visit MikeMichalowicz.com.*

3 Simple Steps To Having A More Productive Day

1. Get the sleep you need. You cannot be productive if you are tired. Sleep is essential for optimal brain function as well as overall physical and mental health. But we all need different amounts of sleep. No matter how much sleep you need, make sure you get it!

2. Block time for specific tasks. Give yourself a set block of time to check e-mail, make phone calls or have meetings. Put each block on your calendar and make sure you aren't being double-booked, then stick with it.

3. No more multitasking. You may have a lot to get done, but you shouldn't double up on tasks or obligations. When you check your e-mail, only check e-mail. When you work on a project, focus on that single project. Research shows multitasking lowers productivity. *Inc., Feb. 18, 2020*

Guard Your Interior

The weakness of any door is that legitimate people need to be able to get in and out. Often, we help people develop a highly secure and functional door to the Internet, but they give little thought to the physical door into their building.

Develop a strategy to verify that service personnel are legitimate with corporate-issued IDs and track visitor movement through the office. Lock the server-room door if it's across the hall from an office that people frequent. Monitor the temperature and whether there is any water in the server room. Consider a closed-circuit camera system.

Think about everyone who has access to your office. The cleaning crew is often forgotten. They spend hours in your office alone around sensitive data. YOU could be left holding the bag if they perform identity theft based on information in your office. It happens every day. Make sure to consider ALL of the office security in your disaster recovery plan and update it regularly.

"We're not ready to declassify that yet. Just label it 'Mum's the Word.'"

WELCOME NEW CLIENTS!

We are thrilled to welcome the following organizations to our family of clients:

WASHINGTON EYE PHYSICIANS & SURGEONS

WILDLIFE HABITAT COUNCIL®

TONGUE Insurance R. K. Tongue Co., Inc.