THE PROBLEM SOLVER

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

What's New

Last quarter, DP Solutions and its staff were incredibly lucky to be able to give back to the community in time for the holidays. The feeling of giving to those who may be less fortunate, and providing even a just little bit of sunshine to their day, simply cannot be measured.

Letter of Thanks for Christmas Donations to House of Ruth "Adopt-a-Family"

Putting together food, water & wellness bags for the homeless.

Volunteering at Goodwill's Annual Thanksgiving Dinner.

January 2019

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

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

5 Fundamental Ways to Protect Your Business from Network Security Risks

As a business professional, you want to create a strong approach to managing the risks within your organization. But there is no need to recreate the wheel. By developing good, strong habits, you can effectively manage security risks by "tweaking" your existing approach, rather than tearing everything down and rebuilding from scratch.

HERE ARE A FEW FUNDAMENTAL WAYS YOU CAN PROTECT YOUR BUSINESS:

1. Establish An Acceptable Use Policy

Many organizations, especially those with a dozen or so employees, lack basic rules on Acceptable Use. It is almost as if they expect users to know what the rules are and what responsible behavior means when using company owned devices and data without formally explaining it to them. It is important that your Acceptable Use policy be extensive, direct, clear, and communicated to staff, so that there is no room for misinterpretation. While we want users to have flexibility with how they use the tools available to them, they need to be aware of what pitfalls to avoid. Simply defining Acceptable Use rules leads to better outcomes and users begin to feel they have a responsibility in protecting the organization's technology assets.

2. **Have A Structured Approach to Maintenance**

If you have technology assets of any volume, then a comprehensive plan to proactively support and maintain the system is necessary. Even in 2019, there are still organizations that merely take a reactive approach to supporting servers, and other sophisticated network equipment, that house significant

Continued on pg.2

Continued from pg.1

amounts of sensitive data. It's almost as if support is a cost they wish to avoid. However, organizations that are not performing any kind of proactive management will often have high severity vulnerabilities. A security incident due to this lack of management costs them much more money and stress than an actively managed system, which has far fewer risks of a major incident occurring.

3. Provide Regular Security Awareness Training To Staff

While having an Acceptable Use Policy is essential, it is also a good exercise to provide some kind of basic education to end users about Security Awareness. The goal here isn't to create a team of network security experts on your staff, but rather give staff some information to identify what incidents they could experience, how to report to management, current trends and how it applies to the organization, and so on. We want people to avoid incidents, but also minimize the damage from potential incidents by recognizing them and responding accordingly.

4. **Perform Regular Vulnerability/Risk Assessments**

Even well maintained systems will have flaws. There are so many potential vulnerabilities, both on the PC/Server level, as well as from the outside, that it is virtually impossible to patch them all proactively. New vulnerabilities are discovered regularly, and even diligent maintenance could

> "There is no need to recreate the wheel. By developing good, strong habits, you can effectively manage security risks by "tweaking" your existing approach."

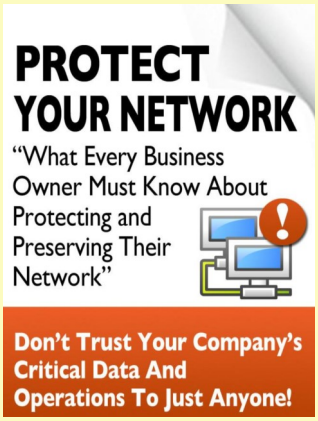
lead to an important patch being missed due to a variety of reasons. Regular vulnerability/risk assessments should be in place so that security issues can be fixed and adjustments can be made.

5. **Make Security/Risk Management A Part of the Discussion During Transitions**

In the rush to execute a new change, like replacing an end-of-life server or implementing a new application, some organizations fail to make security a part of the discussion. It's important to focus on the workflow first. What is it about this particular change to technology that enhances or supports the current workflow? Once that is identified, the next step is to put security tools and policies around that workflow to improve risk management. In order to achieve that, we need to determine what sensitive data this new system handles, and how we want to mitigate the risks associated with it before making big picture changes.

While this is not an exclusive list of ideas and practices to minimize security risks, hopefully it provides you with a line of thinking that you can apply not just to the security risk 'du jour', but also to other risks that have not yet been realized by your organization and the ever changing landscape of security.

Free Report: What Every Small-Business Owner Must Know About Protecting And Preserving Their Company's Critical Data And Computer Systems



This report will outline in plain, nontechnical English common mistakes that many small-business owners make with their computer networks that cost them thousands in lost sales, productivity and computer repair bills, and will provide an easy, proven way to reduce or completely eliminate the financial expense and frustration caused by these oversights.

Download your FREE copy today at
www.dpsolutions.com/ProtectYourNetwork

Welcome New Clients!

DP Solutions is thrilled to welcome the following organizations who recently joined DP Solutions' family of clients:

AACTE
AMERICAN ASSOCIATION OF COLLEGES FOR TEACHER EDUCATION

The American Association of Colleges for Teacher Education (AACTE) is the leading voice on educator preparation. AACTE represents more than 800 postsecondary institutions with educator preparation programs dedicated to high-quality, evidence-based preparation that assures educators are ready to teach all learners.
aacte.org

THE Halle COMPANIES

The Halle Companies, specializes in development, construction and property management of a diversified real estate portfolio throughout the Mid-Atlantic and Southeastern United States.
hallecompanies.com

MCS My Cleaning Service, Inc. Eco-friendly, with you in mind.

My Cleaning Service offers Green Cleaning & Commercial Janitorial Services throughout Baltimore MD, Washington DC and Northern Virginia.
www.mycleaningservice.com

PATRIOT CAPITAL

Patriot Capital is a family of private equity funds focused on debt capital and minority equity investment opportunities in small and medium-sized privately-held companies having minimum annual revenues of $10 million and EBITDA of $3 million.
www.patriot-capital.com

The Most Effective Closing Technique

Of all the things I've done during my entrepreneurial career, selling has been the one constant. Ever since my first job out of college, I had to sell to make a salary. When starting my first business, I had to sell to survive. Even the first book I wrote would have been nothing without a huge selling effort. As a result, I've become a lifelong fan and student of great selling techniques.

My favorite technique used to be the 1-to-10 close. You know, where you ask your customer, "On a scale from 1 to 10, where do you stand on proceeding with us?" And then when they answer, you ask what you can do to make it a 10. The strategy even worked occasionally, despite the fact that it was exactly what I should *not* have been doing.

People resist suggestions. If you're a smoker and I say, "You need to stop smoking – it's bad for you," you'll roll your eyes and say, "Yeah, I know." Then you'll light up a smoke and blow it in my face. We automatically do the opposite of what people suggest.

Later in my career, I stumbled across another 1-to-10 technique, which is still the most effective closing method I've ever experienced. When asking people where they stand on the scale, no matter what they say, I say something like, "I didn't expect you to pick a number so high! From our discussion and your body language, I actually thought you were much lower. Why did you pick a number that high?"

When I suggest a number lower than what they say, people naturally resist my remark and want to go higher. Now they argue about why the number they picked – say five – is not that high, and maybe even change their number to a six or a seven. But no matter what, they're arguing in their own head over why they should go with you.

Tom Sawyer knew this technique. When he acted up and was forced to paint a fence as punishment, his buddies started teasing and ridiculing him. But he just kept painting and said, "Not just anyone can paint a fence." By the time he convinced them that they weren't capable of painting a fence, they began begging him to let them have a try. Only then did he let them, while he relaxed in the shade.

It's a simple strategy, but it works. You can persuade your customers all day to work with you and they won't bite — but get them to convince themselves, and you're in business.

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 www.mikemichalowicz.com.*

5 Sneaky Tricks Cybercriminals Use To Hack Your Network

1. PHISHING. Woe to you and your business if you haven't heard of this one yet. By using an email, chat, web ad or website impersonating a legitimate organization, hackers get members of your team to click and install malware.

2. BAITING. Baiting uses an enticing item to lure employees into giving up personal data, such as a music or movie download or a mysterious flash drive left around the office.

3. QUID PRO QUO. It's like baiting, except that hackers offer a service instead of an item in return for private data.

4. PRETEXTING. This is a type of phishing in which a hacker poses as a respected colleague or member of your organization in order to boost private data.

5. TAILGATING. It occurs when an unauthorized person physically follows your employees into restricted areas.

SmallBizTrends.com, 9/20/2018

Don't Wait 191 Days To Realize There's Been A Data Breach — By Then, It's Too Late

According to a 2017 report by research firm Ponemon, it takes an average of 191 days for a company to realize it's been compromised by a data breach. This number should scare anyone. The longer you take to recognize and respond to a breach, the more criminals can steal and the bigger the damage becomes. What's more, your delayed reaction will leave you fewer options to mitigate the disaster. To survive, you need to stay on top of your cyber security with a team of dedicated professionals keeping tabs on attacks, strengthening your barriers and responding within hours, not days, if the worst ever happens.

SmallBizTrends.com, 10/30/2018

Top Employee Retention Strategies To Keep Your Workers Motivated And Productive

Successful business owners do more than focus on the bottom line. They work to make their office a genuinely enjoyable place to work, creating an environment that fosters loyalty and success in their team over time.

Keeping top performers from jumping ship should obviously be your priority, but these are often some of the most difficult people to keep on board. As they shoulder extra responsibilities and bend over backward to serve your company, they may start to feel undervalued. It's your job as manager to actively seek out any pain points they may be experiencing and resolve them. Regular employee surveys and open lines of communication between teams and management can curb problems before they turn happy workers into disgruntled sandbags.

Of course, no matter how easy you make it for them to do their job, they're going to leave if you still can't give them what they're worth. In a recent Glassdoor survey, it was revealed that over 45 percent of people quit their job because they've been offered more money elsewhere. CEOs tend to be fond of making excuses for avoiding raises and robust benefits, but employees know what they're worth, and they know what they need to stick around.

HomeBusinessMag.com, 10/12/2018