THE PROBLEM SOLVER

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

What's New

Karyn Schell named to The Baltimore Sun's 25 Women to Watch List!

Honoring her leadership in the IT Profession.

Read the full article here:
https://www.baltimoresun.com/features/women-to-watch/bs-fe-women-to-watch-2021-20211020-653k2omlhjfc5cbrwopilxbh4e-htmlstory.html

November 2021

This monthly publication provided courtesy of Karyn Schell, President at 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!"

The Easiest Way To Disaster-Proof Your Cyber Security

Though no one would dispute the increasing prevalence of cyber-attacks on businesses in recent years, many small-business owners believe themselves and their business to be immune to such attacks. Broadly speaking, many small-business owners are likely to think that cybercriminals will go after the bigger fish. However, the fact of the matter is that cyber-attacks are crimes of opportunity, and small businesses often have access to a good amount of sensitive data without many major safeguards. In other words, they're low-hanging fruit, ripe for the picking.

Back in 2019, two-thirds of respondents to a survey about cyber security didn't believe that their small to mid-size business (SMB) would fall victim to a cyber-attack. Consequently, only 9% of respondents said cyber security was a top priority for their business, and 60% didn't have any sort of plan for deterring a cyber-attack. All of this, despite the fact that, according to a report from CNBC, SMBs endured 43% of reported cyber-attacks, and according to data from the Ponemon Institute and Keeper Security, 76% of SMBs in the U.S. alone reportedly endured a cyber-attack within the previous year.

Every small-business owner should have some plan for deterring cyber-attacks so they don't end up as another statistic. Here are a few strategies for keeping the cybercriminals at bay.

Boost Your Cloud Security
Storing data in the cloud is easy and cost-effective, but you should take care to find the most secure cloud storage platforms. Not all cloud platforms make security a priority, but some do. A few of the top-rated, most secure cloud platforms, according to Cloudwards.net, include Sync.com, pCloud and Icedrive.

Secure All Parts Of Your Network
Our computers and the many smart

Continued on pg.2

Continued from pg.1

devices hooked up to our network can become weak spots for hackers to get in. Taking steps to safeguard each device in your network with strong passwords and robust authentication measures will go a long way toward keeping the hackers at bay. In fact, one of the most basic security measures you can take for your network is to restrict access to your WiFi with a strong password.

Invest In Extra Security Measures
Virtual private networks (VPNs) and firewalls are tools that are highly effective in protecting against cyber-attacks, even if they can't prevent 100% of them.

Pay Attention To Updates And Upgrades
When you get notified that one of the technological tools that you use has a new update, it's easy to ignore it. However, you should commit to regularly updating and upgrading these tools because developers will often add patches to their programs that make them more secure against attacks with each update. So, it behooves business owners to regularly install updates for their tech tools.

Back Up Your Data
With one of the most common forms of cyber-attacks being ransomware attacks, where hackers will hold your company data hostage until you pay them a ransom amount, having your company data stored on multiple backups can ensure that your business won't crumble due to your data's inaccessibility.

> **"76% of SMBs in the U.S. alone reportedly endured a cyber-attack within the previous year."**

Limit Employee Access To Your Network
As much as we'd wish it were true, many cyber-attacks don't come from outside of your company. Instead, they originate from within. If you want to limit the amount of damage that someone inside your company can do in a cyber-attack, the best course of action is to limit their access to different parts of your network.

Train Your Employees
At the same time, just as many cyber-attacks occur not because of an employee's malicious intent, but because of their ignorance. They click on a link in a sketchy e-mail and fall for a phishing scheme, volunteer their password info without thinking about it or choose a weak password for their computer. That's why you need to dedicate time to training your employees on best practices when it comes to security.

Set Up A 'Security Culture' At Your Workplace
You need to make cyber security a top priority, not just for your IT department, but for every department at your business. When everyone works together to protect their workplace from a cyber-attack, you have a better chance of actually succeeding.

Will protecting your business from a cyber-attack require a good amount of time and money? Absolutely. Can you afford to ignore the prevalence of cyber-attacks any longer? Statistically, no. The sad truth is that 60% of SMBs that fall victim to a cyber-attack end up shuttering within six months. Don't put yourself in that kind of position. Instead, take your business's cyber security seriously.

Video Offer: 3 Ways to Be Cyber Smart!

There is no better time than now to focus on ways to protect your business and personal life from cyber threats.

Watch this video for three things you can do to be Cyber Smart.

Watch the Video Here:
https://www.dpsolutions.com/dp-solutions-tech-tip-videos

Tech Tip

Patches and Updates address known vulnerabilities…but not the unknown ones

You have probably heard it a million times. Microsoft has discovered a serious flaw in Windows and now you need to install this critical security patch right away.

Of course, being a responsible person, you go ahead and allow the patch to be installed, addressing this specific vulnerability, and making you a little more secure. That's great, but that doesn't mean you should let your guard down.

The reason patches are issued is because a vulnerability was discovered by Microsoft or a third party. But the vulnerability always existed. It existed when the software was published and released for use. It's only now that the community knows about it and can address the problem.

So what else is out there? What are the other vulnerabilities we don't know about?

This is a constant process and not that unusual. A product is released in a state that is finished and working generally, but over time problems are found with it. This isn't all that different from cars that have recalls issued or other imperfect designs in the products we buy and use. The device you are using right now to read this email has some kind of unknown vulnerability on it.

The best thing you can do to deal with this uncertainty is exercise good behaviors:

- Don't click on strange links
- Avoid unknown or suspicious attachments
- Make sure your patch management is solid
- Install anti-malware software to protect you from active threats (among other things).

Your only defense against the unknown is to be vigilant.

Do You Have The Tools To Manage Effectively In The WFH World?

Gone are the days of managers wandering their office spaces, chatting with coworkers and spending time at the water coolers to get valuable information about the state of their teams. With the work-from-home life here to stay for many workspaces, managers must grow beyond their old ways of managing a work team in the office and get used to managing one effectively on Slack, Zoom and whatever other business platforms their company uses.

I believe I have some insights I can offer any managers looking to meet their goals despite only ever communicating with their teams while sitting at home. These insights come in the form of five different questions that, if you answer them affirmatively, mean you're probably an effective online manager.

Do You Set Clear Goals For Your Team?
Unclear goals aren't good anywhere, but at least in a physical office space, team members can clarify the goals with one another in person. That becomes a lot more difficult online, where means of communication can be limited to text messages. As a manager, make sure everyone on your team understands their goals.

Are You Good At Hiring The Right People?
When you hire someone who ends up not being suited for the job, it's pretty easy to tell when you can monitor them at the office. However, if you hire someone for an online remote role, it can take significantly longer to find out if you've made a hiring mistake, meaning you'll lose a lot more time and money.

Can You Delegate Your Work Well?
Delegating tasks in an office means that you can physically see if a team member is taking over those responsibilities. If they aren't, you can always step in and do the project yourself. When you're working from home, however, you'll need to give clear instructions and deadlines, while following up regularly, in delegating tasks to your team.

Does Your Compensation System Reward High Performance?
In a remote context, the forces that push your team to perform at their highest ability don't have as much of an impact. Since compensation and high performance are inextricably linked, a compensation system that directly rewards high performers is the only way that you'll ensure that your team works to the best of their ability.

Do You Follow Through On Doing The Things You Say You'll Do?
Building trust might not take a lot of work in the office, but in a remote setting, communication is key in building two-way trust with your team. When you say that you'll complete a task, complete it – and make sure your team is aware. That integrity, even though you're working from a place where no one can see you, will go a long way in building trust.

Management beyond the office space doesn't have to be a big mystery. If you want to improve your skills in managing remotely, many of our books, such as *Power Score, Who* and *The CEO Next Door*, can help you accomplish that.

Dr. Geoff Smart is the founder and chairman of ghSMART, which helps Fortune 500 companies, CEOs and successful entrepreneurs alike make smart decisions when it comes to curating talented teams. For three consecutive years, Forbes *ranked ghSMART as the best management consulting firm in its industry, and it has produced three best-selling books outlining its principles.*

The Digital-First Economy Is Here

Whether your business is a massive multinational operation or you're a humble "solopreneur," you have now entered the era of the "digital-first" economy. Daunting though it may be to prioritize your business's online presence, there are five traits that will serve your customers well and lead to your success.

Flexibility: Be prepared to constantly advance your knowledge of new technologies and softwares and make changes to your systems when necessary.

Comfort With Outsourcing And Automating: Don't be afraid to delegate tasks, such as fulfillment or marketing management, that keep you from the core work of your business.

Digital Communication Skills: This means not only having the right kinds of digital communication avenues (e-mail, website, social media, etc.) but also knowing how to optimize them to communicate clearly and consistently with your customers.

Understanding Customer Expectations: In a world where customers expect seamless interactions and quick results, make sure you each clearly understand one another's needs.

Cyber Security: Even solopreneurs are at a greater risk for cyber-attacks. Make sure to protect sensitive data in a way that works best for your business model.

How To Handle Digital Identity As A National Security Issue

As we transition into a digital-first economy, the concept of "digital identity," meaning the set of attributes related to your identity that you make known online, should be at the forefront of national security talks. But just how can people, companies, bots and things balance privacy and security in a way that keeps their sensitive information safe?

One way is by prioritizing relevant credentials rather than entire identities. Say you're making an account on a website that you need to be 18 to access. Now, the site could provide you with a way to share your driver's license and credit card information. After all, that would ensure that you are the one using your digital identity on that site. However, if the site gets hacked, then the hackers have all that info about you, when all the site really needed in the first place was your age.

"I always play the GPS throught the backseat speakers. That's where I'm used to receiving instructions."

So, those relevant credentials, also referred to as "entitlements" (because they're the pieces of information that entitle you to certain services), are the best starting point for a discussion about digital identity and national security.

Use This Simple Trick To Make Your Phone More Secure

If you want to protect your smartphone from being hacked, all you have to do is turn your phone off and back on again. Does that sound overly simplistic and cliché? Probably. Does it work? Absolutely.

The reason that simply turning your phone off and on again can thwart hackers is because, historically, hacking has been a game of persistence. Keep at it for long enough, and a person's security protocols will eventually give.

However, with smartphones, hackers have found that they don't need to be persistent because most of us never shut off our devices. Thus, hacking smartphones has become a much more attractive option for cybercriminals.

By simply turning your phone off and back on again regularly, you give cybercriminals far fewer opportunities to hack your device, and they'll likely move on to try and hack a smartphone that stays on continually.

Considering how low-tech this solution is, there's no reason that anyone with a smartphone shouldn't be doing it.