



In This Issue

P.1 4 Questions Your IT Services Company Should Be Able to Say "YES" To

P.2 Is Working From Office More Secure Than Working Remotely

P.2 Top Tips For On How To Prevent Your Smart Cameras Being Hacked

P.2 Top3 Ways to Use MyGlue Password Vault

P.3 4 Questions Your IT Services Company Should Be Able to Say "YES" To

P.3 Do These Things To Prevent Your Business From Getting Hacked

P.4 Four Steps To Move Your Business From Defence to Offence During Times of Disruption



BERTIBRIEF

4 Questions Your IT Services Company Should Be Able to Say "YES" To



Out with the old and in with the new! For far too long, small businesses have taken an old-school approach to IT services and security. In other words, they wait until something goes wrong before they call an IT services company and request help.

Back in the day (think 1990s and 2000s), this approach worked, more or less. External threats, such as hackers and viruses, were still few and far between. A data breach wasn't on anyone's mind. So, it made sense to wait until something went wrong before taking action.

In IT circles, this is known as the "break-fix" approach. Something breaks, so someone has to come in to fix it. And they charge for their services accordingly. If something small breaks and it takes a short time to fix, you could expect a smaller bill. If something big breaks, well, you can expect a pretty hefty bill.

The break-fix approach is 100% reactive. As many businesses have learned, especially in more recent years, as the number of threats have skyrocketed, it can get very expensive. IT specialists are an in-demand field. With just about every business relying on the Internet and Internet-connected devices in order to operate, there's a lot of opportunity for something to go wrong. Continued on pg. 3



Is Working From An Office More Secure Than Working Remotely?

It may come as a surprise but working remotely can be just as (or more) secure than working in the office. *If done right.*

Those are the three operating words: *if done right.* This takes effort on the part of both the business and the remote employee. Here are a few **MUST-HAVES** for a secure work-from-home experience:

Secure networks. This is non-negotiable. Every remote employee should be connecting to a secure network (at home, it should be WPA2 encrypted), and they should be doing so with a VPN.

Secure devices. All devices used for work should be equipped with endpoint security – antivirus, anti-malware, anti-ransomware and firewall protection. Employees should also only use the employer-provided or approved devices for work-related activity. **Secure passwords.** If employees need to log in to employer-issued programs, strong passwords that are routinely updated should be required. Of course, strong passwords should be the norm across the board.

Entrepreneur, June 17, 2020

Top Tips On How To Prevent Your Smart Cameras From Being Hacked

Smart cameras have been under attack from hackers for years. In fact, one popular smart camera system (the Amazon Ring) had a security flaw that allowed hackers to get into homeowners' networks. More recently, Zoom faced a privacy and security backlash as 'zoombombing' became a common vulnerability concern. **Zoom was forced to update their iOS app** and the issue has since been patched, but the risk of being hacked still exists. Here are three ways to keep your camera (and your network) safe from hackers:

1. Regularly update your passwords.

Yes, passwords. This includes your smart camera password, your WiFi network password, your Amazon password – you name it. Changing your passwords every three months is an excellent way to stay secure. Every password should be long and complicated.

2. Say no to sharing. Never share your smart camera's login info with anybody. If you need to share access with someone (such as a family member or roommate), many smart camera systems let you add a "shared user." This will let them access the camera, without the ability to access the camera's configuration or network tools.

3. Connect the camera to a SECURE network. Your smart camera should only be connected to a secure WPA2 encrypted, fire-walled WiFi network. The more protection you put between the camera and the rest of the digital world, the better.

Digital Trends, May 7, 2020

Top 3 Ways To Use My Glue Password Vault

Bad password management is a risk no company can afford. Think securing your password means putting the sticky note under the keyboard instead of on the monitor? **NO!** You probably don't even want to know how users are keeping track of all their passwords. Don't let bad password habits become commonplace in your office. Sharing passwords over email using sticky notes or spreadsheets to track them...it's more common than you think and super risky. With MyGlue, Users Can: store, create, and maintain passwords in a secure app.

You can document and Share your Business Processes & Policies. Document all of your knowledge including SOPs, How-To docs, policies, contracts and more. MyGlue helps businesses reduce onboarding times and increase the efficiency of business processes by making sure that everybody has the tools to perform tasks the right way, every time. Use MyGlue to set up and serve standardized templates as flexible assets.

You can also build checklists to organize your workflow. It always feels **AMAZING** to cross things off your to-do list, right? MyGlue comes with a built-in checklist feature to help your team organize tasks and consistently complete tasks more efficiently. Don't have a project management system? If you adopt MyGlue for password management, your team gets the added benefit of not having to just "wing" their tasks anymore. Yay! A win all around.



Do These Things To Protect Your Business From Getting Hacked

1. Train Employees. Your team needs to know how to identify and handle today's IT security threats. Cybercriminals often rely on your employees' lack of training to break into your network. Ongoing training gives employees tools and resources to overcome this and many other IT security challenges. Make training a top priority!

2. Hold Employees (And Yourself) Accountable. Training and company guidelines don't mean much without accountability. When you set rules, follow them, just as you follow industry and government rules and regulations when operating your business. Be willing to hold anyone who does not accountable.

3. Have A Disaster Recovery Plan. Things happen. When you store sensitive data, you need to have a plan in place to recover and restore that data should anything happen. This doesn't just include data loss from malicious attacks but other types of disasters, including hardware failure, fire and flood. How is your data being backed up and saved? Who do you notify in the event of a breach? Who do your employees call in the event of disaster?

This is exactly why you can't rely on the reactive break-fix model anymore. If you do, you could be putting your business at serious risk. In some cases, the mounting costs and damages done could put you out of business.

If you're hit by a data breach or if a hacker infiltrates your network (which is a common occurrence), what's next? You call your IT services partner – if you have a partner – and tell them you need help. They might be able

to restore lost or stolen data. That is, if you routinely backed up that data. You don't want to find yourself in this position.

And you don't have to.

Instead, take a proactive approach to your IT support and security. This is the new way of doing things! It's also known as managed services – and it's a far cry from the break-fix approach.

If you work with an IT services company that only comes out when something breaks, it's time to get them on the phone to ask them four big questions. These are questions they absolutely need to say "yes" to:

- 1.Can you monitor our network and devices for threats 24/7?**
- 2.Can you access my network remotely to provide on-the-spot IT support to my team?**
- 3.Can you make sure all your data is backed up AND secure?**
- 4.Can you keep our network protected with up-to-date malware solutions, firewalls and web filtering?**

If your IT services partner says "no" to any or all of these questions, it might be time to look for a new IT services partner.

If they say "yes" (or, even better, give you an emphatic "yes"), it's time to re-evaluate your relationship with this company. You want to tell them you're ready to take a proactive approach to your IT support, and you'll be happy to have them onboard.

Far too many small businesses don't bother with proactive support because they don't like the ongoing cost (think of it as a subscription for ongoing support and security). They would rather pay for things as they break. But these break-fix services are more expensive than ever before. When things go wrong, and these days, things will go wrong, you'll be left with the bill – and be left wishing you had been more proactive!

Don't be that person. Make the call and tell your IT services provider you want proactive protection for your business. Ask them how they can help and how you can work together to avoid disaster!

Four Steps To Move Your Business From Defence To Offence During Times Of Disruption

“Everyone has a plan until they get punched in the mouth.” –Mike Tyson

As business leaders, we’ve all been punched in the mouth recently. What’s your new game plan? Since COVID-19, the annual or quarterly one you had is now likely irrelevant.

You have two options:

1. Sit and wait for the world to go back to the way it was, a place where your plan may have worked (and let’s face it, that’s not happening).
2. Create and act upon a new game plan. One that’s built to overcome disruption and transform your business into something better and stronger.

Option 2 is the correct answer! AND we at Petra Coach can help.

At Petra Coach, we help companies across the globe create and execute plans to propel their teams and businesses forward. When disruption hit, we created a new system of planning that focuses on identifying your business’s short-term strengths, weaknesses, opportunities and threats and then creates an actionable 30-, 60- and 90-day plan around those findings.

It’s our DSRO pivot planning process. DSRO stands for Defense, Stabilize, Reset and Offence. It’s a four-step process for mitigating loss in your business and planning for intentional action that will ensure your business overcomes the disruption and prepares for the upturn – better and stronger than before.

Here’s a shallow dive into what it looks like. Defence: A powerful offensive strategy that hinges on a strong defence. Identify actionable safeguards you can put in place. The right safeguards act as the backbone of your company, giving you a foundation you can count on.

Stabilize: The secret to stabilization is relentless communication with everyone. That includes internally with your teams AND externally with your customers. Streamline communication and eliminate bottlenecks through a visual dashboard.

Reset: By completing the first two steps, you’ll gain the freedom to re-prioritize and focus your efforts on the most viable opportunities for growth.

Offence: Don’t leave your cards in the hands of fate. Shifting to offence mode gives you the power to define the future of your business. Equip yourself with the tools and knowledge to outlast any storm.

Interested in a deep dive where a certified business coach will take you (and up to three members from your team) through this process? Attend Petra’s DSRO pivot planning half-day virtual group workshop. (We’ve never offered this format to non-members. During this disruptive time, we’ve opened up our coaching sessions to the public. Don’t miss out!). When you call a time out and take in this session, you’ll leave with:

- An actionable game plan for the next 30, 60 and 90 days with associated and assigned KPIs.
- Effective meeting rhythms that will ensure alignment and accountability.
- Essential and tested communication protocols to ensure your plan is acted upon.

I’ll leave you with this statement from top leadership thinker John C. Maxwell. It’s a quote that always rings true but is crystal clear in today’s landscape: “Change is inevitable. Growth is optional.” Let that sink in.



Andy Bailey is the founder, CEO and lead business coach at Petra, an organization dedicated to helping business owners across the world achieve levels of success they never thought possible. With personal experience founding an Inc. 500 multi-million-dollar company that he then sold and exited, Bailey founded Petra to pass on the principles and practices he learned along the way. As his clients can attest, he can cut through organizational BS faster than a hot knife through butter.