

What's New

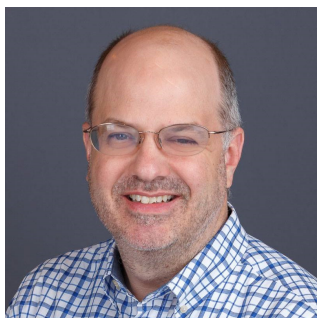
New Year, New Cyber Security Threats!

Have you heard the terms: DarkWeb, Ransomware, Identity Theft? Or, even worse, have you or your company been a victim of them?

We have all heard about the cyber threats that have been on the news lately. However, what you may not realize is that the cyber criminals are silently attacking small businesses banking on the fact that most small businesses do not have proper security in place to prevent them from accessing their network AND it's only going to get worse in 2020 and going forward.

Continued on page 3

January 2020



This monthly publication provided courtesy of Will Sperow, General Manager of Blue Bay Technology.



3 Places You Should NEVER Cut Corners With IT

We all know how easy it is to cut corners in business; we've all done it somewhere. But we also know we shouldn't. You'll eventually have to face the consequences, whether they're small or large. The same applies to IT. When you cut corners, the consequences to your business can be major. Here are three places where you never want to cut costs.

EQUIPMENT

You want to set up a wireless network at the office, but you don't want to spend more than \$50. So, you spend that \$50 and call it good. While this new router may deliver a wireless signal that reaches every employee, you could be making a huge mistake that may cost you dearly.

Routers are a good example of

technology you want to put extra thought and money into. You want equipment that not only makes sense for your business's network needs but will also perform reliably and securely. Cheap routers aren't known for their security features. You want something that will complement the firewalls or security software you have in place (and you *should* have them).

This same idea applies to all other equipment, as well as software. When you cut corners, there's a good chance you'll be opening your wallet again to fix the problem in the near future. On top of that, it puts your data at risk if you're buying cheap, potentially faulty equipment. Do research, ask questions and work with an experienced IT company to make sure your equipment is up to snuff.

Continued on page 2

than you needed to, once for the first investment (on non-scalable tech) and once for the second investment (to catch up with your growth). But because your business has grown since that initial investment, you'll be left with a hefty bill – for much more than you paid the first time. Don't make this mistake!

DATA SECURITY

Just because your data is locked away in the back room doesn't mean it's safe. For one, small businesses are the biggest targets for cybercriminals because most small businesses skimp on data security, making it easy for cybercriminals to steal data and cause a lot of problems.

To make matters worse, if you get hit with a cyber-attack or data breach, it can be incredibly difficult to recover, and many small businesses *don't* ever recover. They struggle for a few months before finally closing their doors.

You need to invest in firewalls, malware protection, data encryption, data backups, password managers and, as mentioned above, good equipment that is designed with reliability and security in mind. And no, you don't have to figure it out by yourself. It can be a lot, and as you dive into the topic of data security, you'll have questions.

This is exactly why you want to pair up with an experienced IT company that specializes in security. It is very hard to run a business and try to be a data security expert at the same time. Thankfully, you don't have to do that. You can get the most out of your equipment, you can be prepared for future growth and you can be ready for the threats to your data! You just have to make that first investment.

GROWTH OF YOUR BUSINESS

Whether you're just getting started or you've been in the business for a while now, you always want to invest in hardware and software that will scale *with* your business. It's safe to say that most businesses want to grow, which means adding more customers and more employees. When that's the plan, scalability becomes a big deal.

Part of it comes back to the first point: cheap equipment isn't typically designed with scalability in mind. It's a quick-fix investment. It's not made for the long haul. Where do you plan on being in five years? What are your growth goals? You have to ask these kinds of questions to determine what kind of investment you need to make, whether it's in billing software, customer service software, workstations or your network infrastructure.

If you don't think about scalability, as soon as you start really growing, you'll be hit by growing pains. You'll have to reinvest in technology, and you'll be spending far more

“Whether you’re just getting started or you’ve been in the business for a while now, you always want to invest in hardware and software that will scale with your business.”

FREE Report: The 8 Most Critical IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime, Data Breaches And

Eighty-two thousand NEW malware threats are being released every day, and businesses (and their bank accounts) are the #1 target. To make matters worse, a data breach exposing client or patient information can quickly escalate into serious damage to reputation, fines, civil lawsuits and costly litigation. If you want to have any hope of avoiding a cyber-attack, you MUST read this report and act on the information we're providing.

Claim your FREE copy today at

<https://www.bluebaytechnology.com/cybercrime/>



What's New

Continued from page 1

Every business needs to start with the basics to secure their data as much as possible. The basics include:

- Firewall, monitoring and management
- Web content filtering
- Spam filtering
- Email Encryption (even if it's not a requirement for your industry)
- Dark Web monitoring
- Endpoint security (anti-virus and anti-malware)
- Cyber awareness training
- Intrusion testing
- Back and disaster recovery plan and testing
- Hire a competent IT security employee or outsource to a qualified managed services company

Even if you do take all of these precautions, you may still be hacked or infected. However, if you take no action to at least employ the basics listed above, you are most certainly going to be hacked or infected at some point.

Today's world environment is fraught with criminals that have the tech savvy to infiltrate your infrastructure with no regards for you, your employees' and your customer's privacy and welfare. To them it's all about how much money they can get in the shortest amount of time without getting caught. On top of that, catching them isn't easy. As a matter of fact, it is extremely difficult.

2020 should prove to be a monumental year of new or amended regulations, federal and state mandates, and industry standards. If you are not already doing "the basics," think long and hard about how it would feel to lose everything you have worked for so long. You might discover that the security of your business is a worthy investment.

5 Keys For Building Effective Multilocation Teams

Technology has made it easier than ever to set up multiple offices around the country, but it also presents new challenges for business leaders: how to build and sustain a positive and productive company culture while managing geographically dispersed teams.

When managing offices in multiple locations, the difference between success and failure often can be traced to the commitment that leaders have in fostering a company culture that embraces open, honest communication, accountability and alignment. Here's how you do it.



1. HIRE RIGHT.

When hiring (or promoting from within) to manage remote office locations, make sure candidates have what it takes to work independently and in a less traditionally structured environment. The nature of working remotely requires team members to be self-starters. They also need to have the knowledge and confidence to solve challenges on their own because they won't be able to walk into your office for guidance.

2. LOOSEN THE REINS.

As a leader, you're ultimately responsible for the success of your team. But once you've hired your team, you have to release control and let team members do their jobs. Establish key performance indicators (KPIs) to set goals, and identify steps required to accomplish those goals, but resist the temptation to micromanage. Warren Buffett said it best: "Hire well. Manage little." This will afford you time to focus on other projects. Not only that, the trust you show will breed loyalty in your team.

3. CONDUCT DAILY TEAM MEETINGS.

Daily huddles provide team members with the opportunity to quickly share their meeting schedules and news that the whole team should hear. Each person can also report on progress toward individual and company quarterly goals and note the top priority for the day. Just because you have an office in another state doesn't mean

those team members shouldn't participate. Morning meetings, even via videoconference, can build team spirit, share information, foster accountability and provide quick solutions.

4. DON'T NEGLECT ONE-ON-ONE MEETINGS.

No matter the size of your organization or the number of remote locations, it's essential for each team member to have one-on-one time with a manager or leader. Absence does not make the heart grow fonder, so hold these meetings at least monthly and preferably biweekly. Implement a system that allows supervisors to track the progress of team members' work, provide a listening ear for any concerns and help them set goals.

5. PUBLICLY RECOGNIZE ACHIEVEMENTS.

As leaders, it's up to us to encourage team members to be the best they can be and to recognize excellent work. Research has shown a direct correlation between workplace appreciation and productivity and engagement. A Salesforce study found that team members who feel their voices are heard are 4.6 times more likely to feel empowered to perform their best work. Create an online kudos board with an app like TINYpulse where you and fellow team members recognize peers for their accomplishments.



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 multimillion-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.

■ Don't Let This Destroy Your Business

Malware can be a confusing word. It covers a lot of different things, including viruses, worms, spyware, ransomware, Trojan horses and more. Malware in any form can destroy data, take control of your computer and cause major headaches.

Most small businesses aren't equipped to handle a devastating malware attack. Even a simple virus corrupting your hard drive can set you back a few days, and that's only if you act quickly to contain and eliminate it. Some forms of malware, including those that scan and steal data from your systems, can end up destroying your business entirely.

Websites and networks are attacked every single day. By some estimates, there is a cyber-attack every 25 minutes – a number that increases in frequency every year. The best

thing you can do is educate your employees about the dangers of malware and prepare your business for an attack. *Small Business Trends*, 10/12/2019

■ 3 Telltale Signs Your Company Culture Is Toxic

1. There's a high turnover. If your business is a revolving door of employees, you've got a big (and very costly) problem. A high churn rate is a clear sign your company culture is broken. It's almost always a top-down issue: management needs to ask themselves what they are doing wrong. If it's not fixed, it can destroy a company.

2. Everyone's confused. Communication is key, and when management can't clearly communicate strategy or they manage behind closed doors, employees suffer. It can lead to serious mistrust between employees and management, and projects are prone to falling apart.

3. Management is purely reactive.

When an employee makes a mistake, punishment isn't the answer. Ideally, it should be a learning opportunity. When managers swiftly react, and suddenly there's a bunch of closed-door meetings, this equals stress for everyone else. If it gets to the point where employees don't bring up problems with the management team, this means there is a complete lack of trust and employees fear the backlash. *Inc.*, 10/20/2019

■ 4 Tips To Successfully Lead Your Team To New Heights

1. Keep communication open (and honest). Whether you talk face-to-face, hold regular meetings or rely on chat software, always have a communication option open between everyone at the company in some capacity.

2. Be willing to delegate. You can't do it all yourself. You hire people with experience to help your business succeed, so let them shine!

3. Anticipate conflict. Conflict can't be avoided, but it can be addressed before it becomes an issue. Train your team on ways to deal with conflict among themselves, with customers and beyond.

4. Embrace mentoring. The best leaders are also mentors to people around them. If someone leans on you for guidance, embrace it! *Business Insider*, 10/18/2019

