PALMTECH
I.T. Solutions For Business

THE LEGAL TECH TIMES

PalmTech Computer Solutions August 2019

3 IT Investments You Should NEVER Skimp On

What is standing between your business's data and hackers a world away? What's your plan when your on-site server fails?

When you skimp on technology and IT solutions for your business, the answers to these two questions are simple: 1) There is *nothing* standing between your business's sensitive data and people who want to take advantage of that data; and 2) There is no plan.

It happens way too often. Businesses cheap out on certain aspects of their technology to save a few bucks up-front. You may even know someone who has done just this. They jump at the chance to outfit their office with a huge monitor and a PC with top specs (even though they don't need it) and then they decide that IT security isn't a priority. They aren't willing to pull out the credit card for a security solution because they don't want to deal with a monthly or yearly cost.

But skimping on security can cost them dearly in time, money, resources and clients. When it comes to investing in IT, here are three things you *never* want to cheap out on.

SECURITY. Far too many businesses – from small to large – underinvest in IT security. We touch on this topic a lot because we see it a lot. These are business owners and managers who fall into the mindset of "It won't happen to me." This is a dangerous line of thinking.

For small businesses, a data breach can be devastating. Not only is data compromised and potentially copied or stolen, but your clients will also immediately question whether or not they should trust you. There's a good chance they end up taking their business elsewhere – and they may even sue you.

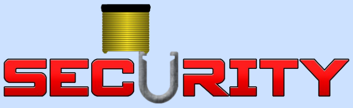
When IT security isn't a priority and you invest in the cheapest option available, it's like asking hackers to let themselves in. One study by the security firm

continued on page 2

Don't Miss Our Cyber Security Talks!

We periodically will present and discuss cyber security and The Dark Web, as it affects you and your business. Take a look at our upcoming events!

www.palmtech.net/events/



This monthly publication provided courtesy of Chuck Poole, President of PalmTech Computer Solutions.

Our Mission

To equip small and midsized businesses in the West Palm Beach area with a smooth running and seamless IT platform that enhances productivity, improves efficiency, and creates a competitive advantage.

Imperva found that over 50% of all Internet traffic is made by bots. Many of these bots are looking for security holes. They test websites and networks, looking for a way in. If they find their way in, they can do some serious damage.

Investing in solid IT security – with an experienced team of IT specialists behind that security – can prevent that damage from ever happening in the first place. It's not only about protecting your business assets but also protecting your clients and giving them another reason why they should trust you.

BACKUPS. You keep all of your data on-site with no backups. It's all stored in one central location and that's it. This is a recipe for disaster if you get hacked, but it can be an even bigger disaster if a hard disk or server fails.

Suddenly, you find yourself unable to access client information, invoices, phone numbers – you name it. Having a backup on-site or in the cloud means everything you do has an extra layer of protection. A backup gives you the ability to restore your data should the worst-case scenario occur.

It's even better to go a step further and have a backup for the backup. Have one on-site solution and one cloud-based solution. Even if the backup to the backup is as simple as a 4TB hard drive from Amazon, it has the potential to save your business should anything go wrong.

Of course, you also need a system in place to make sure data is being regularly and accurately updated. Another mistake businesses make is buying a backup or backup services, but not making the best use out of it. For example, they simply never bother to set it up. Or it is set up but isn't configured correctly and isn't backing up data as intended – or is backing up data too infrequently to be useful.

> **"... when you cut corners and cheap out, you will end up paying for it later..."**

UPDATES. How old is your technology? Think about the hardware you're running – and the software on that hardware. Letting your technology fall behind the times can spell trouble. Not only are you opening yourself up to security vulnerabilities, but you may also be operating on technology that's no longer supported by the developers.

If the developers are no longer publishing updates or supporting the software, this is a huge security red flag that you need to update. On top of that, should you or an employee need to troubleshoot a piece of unsupported software, you may find yourself going up against walls. There might be no one to call, and if a Google search doesn't help, you may be out of luck.

The potential headaches don't end there. If you're running unsupported software on shiny, new hardware, you may be voiding the warranty of that hardware (always check your warranties and the fine print of any hardware you buy).

Alternatively, if you're trying to run brand-new software on old hardware, chances are you're going to run into compatibility issues. That wonderful piece of software might not work, or work the way you expected it to, all because you didn't want to update your old hardware.

It's not always fun to reach into your pocketbook to invest in good IT security, cloud backup storage or new hardware, but when you cut corners and cheap out, you will end up paying for it later, one way or another. When that bill comes, it's going to be a lot bigger than if you had committed to those IT investments in the first place. Call PalmTech at (561)969-1616 for information on how we can help secure your network.

Shiny New Gadget: Drone X Pro

People are constantly looking for creative ways to express themselves, document their daily lives, share their adventures with their loved ones, and immortalize the most precious memories... Nowadays, it's not so easy to stand out from the crowd, but there's finally one assured way to do it – and we call it DroneX Pro!

DroneX Pro was created with simplicity in mind so that everyone could use it. There's no need for heavy, bulky devices anymore – DroneX Pro's well-thought-out and ultra-compact design allows you to carry it wherever you go since it can easily fit in your pocket! Despite its size and portability, DroneX Pro provides you with the most valuable features of high-quality drones and turns the process of taking pictures into an incredibly fun experience!

Capital One Breach: What You Can Do Now

A data breach to Capital One servers in March exposed the personal information of nearly 106 million of the bank's customers and applicants. The hack, which included US and Canadian customers of the banking and credit card company, followed the settlement reached between Equifax and the Federal Trade Commission concerning a hack in 2017 that affected 147 million customers.

According to Capital One, the breach on March 22 and 23, 2019, resulted in the hacker gaining access to personal information related to credit card applications from 2005 to early 2019 for consumers, applicants and small businesses. Capital One detected the breach on July 19. Among the personal data exposed were names, addresses, dates of birth, credit scores, transaction data, Social Security numbers and linked bank account numbers.

About 140,000 Social Security numbers and 80,000 linked bank account numbers were exposed, Capital One said. And for Canadian credit card customers and applicants, approximately 1 million Social Insurance Numbers. Capital One said, however, that no credit card account numbers or login credentials were revealed in the hack.

Capital One said it will contact by letter U.S. individuals whose Social Security numbers or linked bank account numbers were part of the hack. Affected individuals can probably expect to hear the week of August 5. At the moment, Capital One doesn't have a website that lets you check for yourself, unlike with the tool Equifax released to see if you were part of its data breach.

Be on guard for emails and phone calls from scammers posing as Capital One or government representatives asking for credit card or account information, your Social Security number or other personal information.

Monitor your credit reports. Look for unusual or unfamiliar activity, such as the appearance of new accounts you have not opened. In addition, sign up for a credit monitoring service.

If you suspect fraud, place a fraud alert with each of the credit reporting companies: Equifax, Experian and TransUnion. You will also need to contact fraud departments for each company, freeze your credit and DOCUMENT EVERYTHING. — cnet.com

Are You Prepared For Hurricane Season?

Even if you feel your business is not likely to face the brunt of a hurricane's landfall, you should take steps to prepare for hurricane season. With talk of a busy hurricane season ahead, it is important that any business which might face heavy storms takes extra precautions. Extreme weather of any kind, from tropical depression and storms to Category 5 hurricanes and tornadoes, can not only cause structural damage to your business, but can also cause catastrophic data loss and network damages. Visit www.palmtech.net/hurricane-prep/ to download our Extreme Weather Checklist!

4 Reasons CEOs Should Plan For Failure And Encourage Risk-Taking

Every successful company leader will tell you that failure is a part of business, but far fewer will admit they plan for failure. Growing a business requires taking risks, and failure is a frequent outcome on the journey to achieving success.
In their best-selling book Switch, co-authors and brothers Chip and Dan Heath describe how world-renowned design firm IDEO (perhaps best known for its work with Apple) plans for failure during its design process. The company's designers even created a process chart that factors in the excitement and hope at the beginning, the emotional lows of when things aren't going as planned and the joy of victory at the end.

It's a brilliant way to view risk-taking and how leaders can plan for failure while on the road to success. It's an approach I embrace at Petra Coach and recommend to the member companies that we consult. Here's how you do it:

1. Plan For Failure By Knowing The Risks: When taking a risk, make sure it's a calculated one. Evaluate the upsides and downsides and what they mean to your business. Have answers to key questions like: does the undertaking align with your company's vision and mission? Do the activities and tasks support company goals and priorities? Did we plan for failure, and do we know how to respond if things go sideways? Remember, a failure that is aligned with your business's goals is still a step in the right direction.

2. Learn From Your Mistakes: Every failure experienced will provide important lessons that can be applied to your business. Roll up your sleeves and find out what went wrong. Were your expectations incorrect? Did you misjudge market demand? Was your strategy not on target? Be brutally honest about the hows and whys, but don't dwell on it or point fingers. Get your team together to determine the necessary changes and move forward.

3. Celebrate Failure: Failure is part and parcel of running a business, so don't feel ashamed when things don't go as expected. Failure means you're taking action to grow your business. Celebrate each failure by publicly applauding team members who had the courage to take a chance and accept the consequences. Hold a "failure party" or create an award for the biggest risk taken. It will foster a positive attitude toward smart risk-taking.

4. Encourage Open Discussion About Failure: All business leaders have failed at some point during their careers. To foster a culture of smart risk-taking, encourage team members to share their highs and lows about projects where they took a chance. Make it acceptable to talk about mistakes so team members are encouraged to share their experiences and ideas. It will create a more open and creative environment and help build healthier teams.

In today's world where business seems to move at the speed of sound, the biggest risk is not taking any risk at all. Few, if any, business leaders have succeeded by sticking to their original idea. A planned, detailed strategy to deal with failure will keep your team energized and in a positive mindset when they tackle the next big idea.

About the Author: As the founder of Petra Coach, Andy Bailey can cut through organizational BS faster than a hot knife through butter, showing organizations the logjams thwarting their success, and coaching them past the excuses we all use to avoid doing what needs to be done. Andy learned how to build great organizations by building a great business, which he started in college. It then grew into an Inc. 500 multimillion-dollar national company that he successfully sold and exited.

Are Your Credentials For Sale On The Dark Web?

Visit www.palmtech.net/darkweb/ For A Free Scan!