



# Newsletter

## What's Inside

3 IT Investments to Never Skimp on  
*page 01*

4 Reasons CEOs Should Plan for Failures  
*Page 02*

3 Things Every Business Needs to be Successful  
*Page 03*

Featured Products & Monthly Tech Tip  
*Page 04*

## 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 upfront. 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 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 them. 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.

**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

Contact RJ2  
(847) 303-1194

Corporate Office  
1900 East Golf Rd.  
Suite 600  
Schaumburg, IL 60173

Chicago Office  
333 S. Wabash Ave  
Suite 2700  
Chicago, IL 60604

## 4 Reasons CEOs Should Plan for Failure

**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 how's 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.

### FEATURED PARTNER



## Mimecast

Cloud-based Email Management

Mimecast cyber resilience provides email cloud services for security, archiving, and continuity. Protect your email system without compromise.

## RJ2 SPOTLIGHT

# Joel Pabst

## Database Administrator

Joel Pabst has been a part of the RJ2 team since 2012. He recently graduated from Trinity International University- IL, where he studied Pastoral ministry. He started as a Jr. Recruiter for the company before moving to Database Management. Since graduation, Joel has not only continued his responsibilities but also assists in areas of Marketing, Documentation, and Accounting.

Fun Fact: Joel enjoys long walks on the beach and attending concerts with friends.



## BUSINESS PRESENCE

## Do You Have These 3 Things Every Business Needs to be Successful?

***You have a solid team. People are everything in business – that includes your employees. You strive to hire the best team (who match your core values and company culture and who bring top-notch skills to the table) and you train them well (they understand your systems and processes). On top of that, they're happy!***

You have **purpose** behind what you do. We all need purpose to not only be happy but also to thrive. When your team knows what they're working toward and understand the value of their work, that gives them purpose. You've clearly laid out the objectives, and everyone is on the same page. When your employees know why they do what they do, they're happier and more productive for it.

You are **passionate**. You don't just love what you do, you love the people you work with, and you love the difference your business makes in the community or the world. When you have passion,

it's infectious. It inspires people around you. When your team is inspired, they'll go the extra mile, and your business will find success like it's never found before. Inc.com, 5/20/2019

With so many access points, from cell phones to laptops and home computers, how can anyone hope to keep their network safe from hackers, viruses and other unintentional security breaches? The answer is not "one thing" but a series of things you have to implement and constantly be vigilant about, such as installing and constantly updating your firewall, antivirus, spam-filtering software and backups. This is why clients hire us – it's a full-time job for someone with specific expertise (which we have!).

Once that basic foundation is in place, the next most important thing you can do is create an Acceptable Use Policy (AUP) and train your employees on how to use company devices and other security protocols, such as never

accessing company e-mail, data or applications with unprotected home PCs and devices, for example. They will also learn how to create good passwords, how to recognize a phishing e-mail, what websites to never access, etc. NEVER assume your employees know everything they need to know about IT security. Threats are ever-evolving and attacks are getting more sophisticated and cleverer by the minute.

If you'd like our help in creating an AUP for your company, based on best practices, call us at 847-380-3430. You'll be glad you did.

# Featured Products

## RJ2's Most Popular Mimecast Package:

### Mimecast MSA - Integrated Security, Email Continuity & Archiving

Mimecast extends traditional gateway security to defend against malicious links in email, weaponized attachments and malware-less social-engineering attacks, often called whaling. An independent archive makes key information rapidly accessible to employees and administrators. Sensitive information is safeguarded with content control and content blocking. And in the event of on-

premise or cloud service email outages, Mimecast Continuity keeps employees productive – right from everyday applications and devices they use every day.

Call RJ2 today if you would like to hear more about our other packages we offer!

# August

"Technology is a useful servant but a dangerous mast"  
-Christian Lous Lange

## Tech Tip of the Month:

### End of Life for Microsoft Applications:

- SQL Server 2008R2 - 7/9/2019
- SQL Server 2008 - 7/9/2019
- Windows 7 - 1/14/2020
- Exchange Server 2010 - 1/14/2020
- Windows Server 2008 R2 - 1/14/2020
- Windows Server 2008 - 1/14/2020

These end of life dates are coming up in a few short months, are you prepared? Call RJ2 today to get started!

