



NEW! RIT Referral Program

We appreciate the opportunity to serve you and your referral is one of the highest compliments we could receive. When you refer someone to Reliable IT, you trust us to deliver superior levels of quality and service to a company you respect as well.

We value your trust, and as a way to demonstrate our commitment and appreciation for your referrals, we offer this incentive to our clients:

Introduce us to a new prospective client and if that client signs a contract for services, you will receive the amount of their first monthly fee (minus 3rd party costs) credited to your company's statement for Reliable IT services (up to one month of Free services) on your next bill.

For More Information, please contact: Aaron Biehl at 866.634.3230 or Abiehl@RITBanking.com



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 Imperva found that over 50% of all Internet traffic is

August 2019



This monthly publication provided courtesy of Aaron Biehl, Chief Operating Officer, Reliable IT Banking.

We are a 24-year-old SOC 2 Managed IT, Security and Compliance Provider for Community Banks Nationwide. We provide monthly support to 40+ Community Banks representing 4500+ devices under management. Our standard of excellence includes personalized attention with a dedicated team, 24/7 live answer/monitoring, & on-going innovative engagements with your key stakeholders to ensure IT is effective, secure, and accelerates growth.

Continued on pg.2

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.

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.

“... when you cut corners and cheap out, you will end up paying for it later...”

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 likes it's never found before. *Inc.com, 5/20/2019*

WHAT THE HECK IS AN AUP ... AND WHY DO YOU WANT IT?

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 clever and sophisticated by the minute.

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

 RELIABLE IT
BANKING

EXECUTIVE SUMMIT

**Join us on October 25th, 2019 for the
Reliable IT Banking Executive Summit at
The Hyatt Regency Huntington Beach Resort & Spa**

Registration for the Reliable IT Banking Executive Summit is Now Open!

Take advantage of a great opportunity to connect with peers and bring yourself up to date on the latest trends and technologies available to Banking Professionals.

You will get inside knowledge on the latest advances in Banking IT, helping you to innovate, increase revenue, decrease costs, and assist in providing the best possible Customer Care and Experience.

This is a FREE event for you! Reliable IT Banking will also provide your meals during the conference.

**Our agenda for this event will include in-depth discussion
and presentations on topics such as:**

- ✓ Security for Banking
- ✓ Staying Compliant with GLBA and BSA
- ✓ Business online reputation management
- ✓ Cloud-based Solutions for Banking
- ✓ Analytics for Banking
- ✓ Business process improvements and management

Register for the Reliable IT Banking Executive Summit at:
www.RITBanking.com/attendee-registration/

We look forward to seeing you in October!

You are Invited!

RIT Banking Executive Summit on October 25th, 2019



PRSR1, STD
U.S. POSTAGE
PAID
RANCHO CORDOVA
CALIFORNIA
PERMIT NO. 361



RELIABLE IT
BANKING

1540 Main St.
Suite 218, #107
Windsor, CO 80550

Inside This Issue:

- 3 IT Investments You Should NEVER Skimp On | 1
- Do you have these 3 things every business needs to be successful? | 2
- Reliable IT Banking Executive Summit | 3