INDEVTECH

TECHMinutes

Your Small Business Technology Information Source!

This Issue:

Vendor Management is Easier with Managed Services

Every business has vendors and most of them take up more time than they probably should. Some of the relationships are pragmatic and fulfilling, but many take up too much time and effort and tend to distract decision makers from focusing on what is truly important within the business. As far as technology goes, depending on your company, you may have...

Read the Rest Online!
https://bit.ly/3DXCxGK

About Indevtech Incorporated

We are the IT department for many small businesses in Hawaii, across different verticals such as healthcare, legal, financial, and manufacturing concerns.

Visit us **online** at:
newsletter.indevtech.com

Indevtech Celebrates 21 Years Serving Hawaii

I started Indevtech in my parents' basement, with $1,000 in capital. Most of that went to pay the attorney's fees! Back then, we exclusively provided graphic design and custom web development services. Over the years we have evolved with the times, and today we are the IT department for many local businesses. I get nostalgic this time of year, thinking of where we came from and all that's yet to come. It is a good time to pause and say thank you to those companies and individuals who have helped us become who we are today. Thank you for being part of Indevtech's journey for 21 years, and we are delighted to be a part of yours. - Scott Cooley, President

Cybersecurity is a Multifaceted and Strategic Issue for Small Businesses

There are a lot of threats out on the Internet, and many of them have absolutely a slim chance to threaten your business. Unfortunately, there are plenty that can and it only takes one to set your business back. Many IT professionals currently working for enterprise businesses deal with threats day-in and day-out, so they are experienced and knowledgeable. Small business owners, who for all intents and purposes are the lead IT decision-makers, don't always consider these risks; they just need to keep their business running effectively.

Some Interesting SMB Cybersecurity Statistics

Statistics taken in context can provide a good deal of perspective. Here is one that will surprise most people:

- The average cost to a small business from a cyberattack that is mistakenly initiated by an employee, partner, vendor, or someone else associated with the company is over $7.5 million per incident for companies with under 500 employees.
- Over two out of every five small businesses don't have any type of cybersecurity plans in place.

(Continued on page 3)

91% of IT Professionals Are Torn Between Security and Business Continuity

When it comes to your business, what do you prioritize? Do you focus more on security, or do you focus more on the business continuity side of things? The reality here is that both are of critical importance. Unfortunately, however, it seems that many executives feel like the current circumstances surrounding the ongoing COVID-19 pandemic have led them to prioritize one over the other.

A survey published by HP Wolf Security showcases that many IT professionals feel like they have had to prioritize business

(Continued on page 2)

Here are 4 Tips that Will Help You Get More Done

You don't need us to tell you that business owners have a lot of work to do, so you should make it a priority to streamline as much of this work as possible. You can use an easy four-step process to make your day-to-day tasks easier and more efficient, and who knows? You might even be able to free up some of that time by asking others to pitch in every now and then. Here are four tips you can use to get the most out of your productivity routine throughout the day.

Sit Down and Plan Your Day Out

First, you will want to get a preemptive start to the day by ironing out tasks that must be done. Essentially, you are building a plan before you leave your office the day before. This lets you hit the ground running when you get to the office or log on to your computer the next day. You don't have to question how you are going to spend your time; you know exactly what needs to get done.

Break Large Tasks Into Chunks

It's not always as simple as having a checklist of things to do, and in the case of larger projects, you can break them down into smaller, more manageable chunks. By focusing on tasks in a more self-contained way, you can ensure that you are dedicating all of your attention to them rather than getting derailed from the major project whenever something small happens that distracts you from the task at hand.

When In Doubt, Delegate

We bet that some of your tasks can be delegated to other staff, so if you are not actively using this skill to make your life easier, we highly recommend doing so. Delegating tasks takes them off of your plate and gives whoever is delegated a sense of ownership of the task, which can be a powerful motivator in its own right.

Outsource When Possible

Depending on the type of business you run, you will likely specialize in certain tasks. So, what do you do for tasks that you are not a professional in? This is where outsourcing comes into play. Why worry about what you don't know when you can rely on other professionals who do know it? In particular, IT and business technology are great ways to get value from outsourcing and take your productivity to the next level.

To help you with delegating tasks and outsourcing, Indevtech offers comprehensive managed IT services that can help you make your life easier and less stressful. To learn more, reach out to us at (808) 529-4605.

Share this Article!
https://bit.ly/3IOFIEj

91% of IT Professionals Are Torn Between Security and Business Continuity

(Continued from page 1)

continuity over the security of their infrastructures. This is not some insignificant number, either; the vast majority—91% of respondents, to be exact—have been pressured into focusing more on business continuity, i.e. keeping operations running--rather than prioritizing security. In a work environment where remote work is slowly becoming the norm, this is a dangerous trend, and one that could have dangerous consequences.

Other notable numbers include the following:

- 76% feel that security is placed on the backburner rather than being a priority.
- 83% feel that their organization's security is becoming a "ticking time bomb," as in it's only a matter of time before something goes horribly wrong.

Considering the relationship that many workers have with security precautions, it's no wonder that these concerns are present in such a capacity. The same survey indicated that younger workers in particular are more likely to find ways around security so that they can get the job done in the most efficient way possible. 48% of respondents claimed that these security measures got in their way, and 31% found themselves trying to circumvent them entirely.

This negative connotation that many workers have with security precautions extends far beyond just younger employees, though. In general, 48% of workers found that security measures seem to just waste their time, and 54% of the 18-to-24-year-old category were more concerned with meeting their deadlines and getting the job done than with the security of their systems. Furthermore, a shocking 39% of respondents claimed that they did not know anything about the security policies for their organizations.

We know what you are thinking; it does not matter what the employees think, as long as the systems are secured. While there is some truth to this statement, there is value in considering the relationship that your employees have with this security technology so that they are more likely to buy into the security...

Read the Rest Online!
https://bit.ly/3m4EwTl

Cybersecurity is a Multifaceted and Strategic Issue for Small Businesses

(Continued from page 1)

- Nearly one out of every five small businesses experience some form of cyberattack every year.

What Are You Spending on Cybersecurity?
With those statistics in mind, it is prudent to come up with a plan that will help keep you from dealing with a data breach, a malware attack, or any other negative scenario that could happen as a result of getting hacked. Here are three strategies that can help.

Invest in Employee Training
The majority of today's cybersecurity problems have at least a little to do with your employees. Phishing attacks are the most utilized hacks and they require someone from your organization to take steps to provide access. You need to train your employees how to identify and report suspicious emails, calls, and instant messages; and, how to utilize company technology without exposing data and other digital assets.

Vet Your Vendors and Partners
Another common problem occurs when you utilize a service or have agreements with a third-party company or vendor. If that organization gets hacked, it could have an immediate effect on your business. Many of today's small businesses utilize cost-effective cloud solutions that may not be secure enough in their own right. If you are going to utilize hosted solutions to run your business, you should consider hosting them with reputable vendors. Indevtech can help you make the right choice.

Keep Your Network Managed
The best thing any company can do is just to deploy tools to secure their network and to keep those tools managed and maintained consistently. Here are a few suggestions:

- Keep all network-attached devices patched and up to date.
- Use automation to verify configurations, and to detect unauthorized changes that happen on your network.
- Utilize two-factor authentication on all applicable software and encryption where possible.

There are many more solutions to the cybersecurity problem, but it is a strategy that has to be consistently utilized because it only takes one instance to really cost your business.

Talk to one of our IT professionals about cybersecurity or any other technology issue, give us a call today at (808) 529-4605.

Share this Article!
https://bit.ly/3IPHYer

Checking Out a Professional Data Backup Strategy

Data backup is extremely important for any business, but some companies struggle to implement this solution in an effective way. First, we'll outline some of the information you should know about data backup, then we'll dive into the details on how to successfully implement a data backup solution.

What Data Should Be Backed Up?

Your business might store a ton of data, leading your organization to make some questionable decisions regarding which data should be backed up. The general consensus is that you shouldn't back up and restore all of your data all at once; rather, you should prioritize data that is important to your operations which will allow you to keep them up even under the worst circumstances. Once you have identified the minimum amount of data your organization needs to sustain an acceptable level of operations, you can then push your efforts toward restoring the rest of your data over time.

How Often Do Backups Occur?

Data backups used to happen only once or twice a day through tape backup, and it was an incredibly resource-intensive process that could not happen during the workday. You should prioritize backing up data that has been changed recently rather than files that simply exist in the background. Doing so allows you to perform backups much more often. We tend to prefer 15 minute intervals if possible.

Where Do the Backups Get Stored?

We recommend that you use the 3-2-1 rule for your data backups. This means three copies of your data total, stored in two physical locations, one of those locations being offsite, like in a secure cloud environment. You shouldn't store all of your backups in one location, either off-site or on-network, because if anything happens to that particular location, your chances of recovering from a data loss incident are decreased considerably.

Where Does the Backup Deploy To?

You should have a plan in place for every possible kind of disaster, even one that completely destroys your in-house infrastructure and renders it inoperable for the foreseeable future. Some data backup systems come equipped with hardware that can function as a temporary server should the rest of your infrastructure fail, and it can keep your business going until a replacement has been secured.

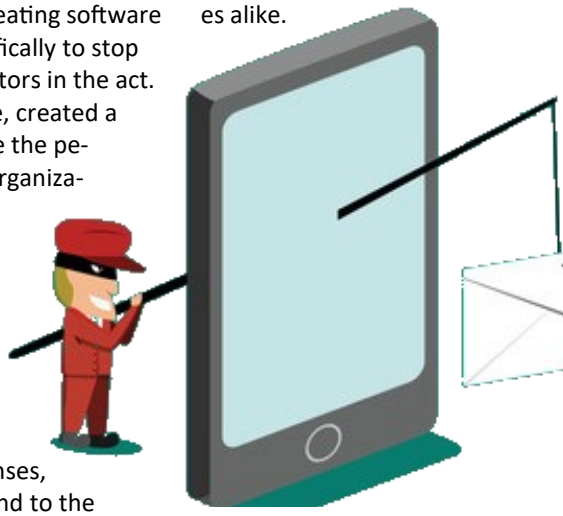
Indevtech can aid your business in implementing business continuity and data backup solutions. We can even automate the entire process, taking a significant amount of frustration and stress out of the equation entirely. To learn more, reach out to us at (808) 529-4605.

Share this Article!
https://bit.ly/3m5FdMf

The Dangers of Near-Constant Phishing Attacks

For twenty years, hackers have tried to breach organizational networks by finding or breaking holes in the network's perimeter, or in exposed servers. This led to the cybersecurity industry creating software designed specifically to stop these threat actors in the act. This, in essence, created a situation where the perimeter of an organization's network was extremely hard to breach. The problem was that as soon as something was able to get through the outer defenses, there was no end to the devastation a hacker could cause inside a network.

This caused a shift in the way that hackers went about their dastardly business. Since they couldn't gain access the "old-fashioned way" they needed a new strategy. As a result, using the resources at their disposal, hackers began to use people with access to the network to let them in. This strategy, sometimes called social engineering, created deceptions that pulled the wool over users' eyes and provided exactly what they were looking for: a way in. Today's hacker has his/her sights firmly targeted on the users of the secure computing network and it is leading to unprecedented levels of devastation for users and businesses alike.



What Is Phishing?

The strategy is as old as war: if one avenue of attack is blocked, you have to try and attack the flanks. In this case, the flanks are the users that have access to a network. You see, users are susceptible to all manner of different ploys. Hackers get them to click on links for free software, they masquerade themselves as people in authority, and they send people direct messages that only the well-trained person would ignore and report. Additionally, some users type their personal access credentials into fraudulent forms. The phishing attack is one part fraudulent scam, and one part belligerent lack of diligence. Together, these two problems can be trouble for your business.

A phishing attack can come at any time and can affect any organization. This is because hackers flood email, instant messaging, or any other method of computer-based communication to expose as many people as possible. No matter what industry you work in, there is a very strong chance that your organization is being phished at this very moment. That's mainly because most phishing messages are sent in mass campaigns designed to flood so many inboxes that the chances that someone makes a mistake are extraordinarily high. In fact, over 90 percent of businesses and nonprofits have seen phishing emails over the past two calendar years...

Read the Rest Online!
https://bit.ly/3IUsw0P

Indevtech has been serving Hawaii since 2001, providing end-to-end managed IT services to small- and medium-businesses. Our philosophy is very simple: we strive to be the best at what we do, so that you can succeed at what you do. We have a proven framework that, when deployed with a solid commitment from our clients, provides an unshakable foundation on which our clients can build their businesses.

Tech Trivia
According to Internet Live Stats, Iceland has the highest Internet penetration rate of any other country at 100%.

Indevtech Incorporated

Pacific Guardian Center, Mauka Tower
737 Bishop Street, Suite 2070
Honolulu, Hawaii 96813-3205
Phone: (808) 529-4605

newsletter@indevtech.com

blog.indevtech.com

Visit us **online** at:
newsletter.indevtech.com