INDEVTECH

TECHMinutes

Your Small Business Technology Information Source!

This Issue:

4 Means of Improving How Productive Your Team Can Be While Mobile

Mobile computing has become a crucial part of many businesses. Unfortunately, it isn't always cut and dry as far as the use of these devices is concerned. Sure, they have proven to be a useful tool, but they also have been known to cause significant distractions. If you are looking for a way to maximize the benefits of mobile computing, these four tips...

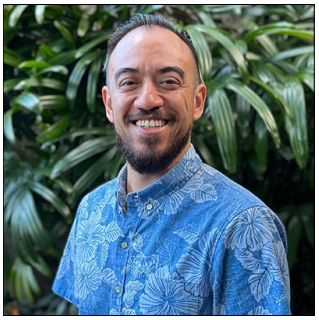
Read the Rest Online!
http://bit.ly/3l8cU2M

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

Employee Spotlight: Eric Newhouse



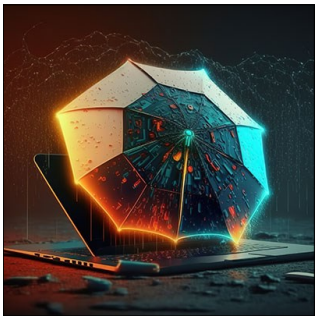
About Me: I'm a Kauai native now residing on the island of Oahu. I've held a passion for computers ever since I was a kid with my family's Macintosh Performa and Windows 98 PC. I originally combined that passion for computers with my love for art and set out on an initial career in graphic design. It was a nice, balanced split between my left and right brain, until my left brain took over and eventually led me into the IT world.

I now have almost nine years of experience in IT, with roles ranging from application administrator to service desk manager, and I love every minute of it. I find the biggest satisfaction in helping users solve their problems, whether it be something that's not working as it should, or a process that can be made more efficient, giving the user peace of mind and more time in their day.

I'm excited to advance my career in IT with my Centralized Services Manager role at Indevtech, utilizing an array of tools to monitor and deliver a proactive approach to the

(Continued on page 3)

Insurance Companies are Starting to Require Cybersecurity—What Do I Do?



Cybersecurity is quickly becoming one of the leading risks that businesses of all shapes and sizes face. Cyberattacks are expensive, they risk your continuity, and they could even get you in hot water when it comes to compliance regulations, local and state regulations, and virtually any entity you are associated with.

It might feel like this is an insurance company's way to nickel and dime business owners, as premiums will continue to rise, especially for businesses that aren't meeting certain requirements, but the truth is, with so much risk, the entire world needs to adjust for cybersecurity.

Why is My Insurance Company Talking to Me About Cybersecurity?

This is essentially happening for most businesses, no matter where you are, and no matter what industry you are in. There are going to be some exceptions—businesses and organizations that are in the healthcare or financial services fields, as well as a handful of other industries that typically deal with more sensitive information, then they might have higher standards, but generally, in order to provide coverage for a business they want that business to be taking minimal steps to ensure that your business isn't wide open for a cybersecurity attack.

What Cybersecurity Requirements Does My Business Need to Meet?

Your insurance provider will typically give you a list of the things they want you to have. That list will likely include the following things:

- Secured, encrypted data backups
- Strong password policies
- Multifactor authentication
- Email filtering

(Continued on page 2)

Are Your Password Practices Falling Short? Let's Build Them Up

When it comes to your business' cybersecurity, passwords are a pretty critical part of the system. This means that making sure they are secure is just as critical…however, that is not to say that this is easy. We, however, wanted to make sure that creating sufficiently secure passwords for all of your accounts is a far simpler prospect by the time we're finished here.

What Password Best Practices Do We Recommend?

Here's a quick list of some of our usual suspects:

- **Keep them complex:** Fill your passwords with upper and lower-case letters, numbers, and special characters.
- **Longer passwords are better:** The longer a password is, the more likely it is that an attacker will get it incorrect. Do your best to create memorable, not guessable, passwords.
- **Use passphrases instead:** Passphrases are effectively the upgraded version of a password, as they are far harder to guess while much easier to remember.
- **Use a unique one for each account:** Let me ask you this…would you rather one of your accounts be breached, or all of them? Using a different password for each protects all of your other accounts.

These practices will result in more complex passwords, which will be inherently more secure. On top of these, there's still more you can do to keep your various accounts safe.

Other Means of Protecting Your Accounts

Some additional practices and technologies take the above precautions to the next level. Implementing multi-factor authentication and utilizing a password manager helps you get the most out of your passwords.

Multi-factor authentication calls upon additional authentication protocols to ensure your security. By requiring a user to provide an additional proof of identity—whether that's a second password or PIN, a physical hardware key, or biometric scan—MFA makes your account far more secure.

Password managers help make the "different password for each account" practice far easier to manage. These tools store your passwords behind encryption and a single master password, allowing you to store and automatically populate your credentials as needed. These tools can even assist you in creating secure passwords to use, truly making proper security the easy option.

Share this Article!
https://bit.ly/3Lm6sjj

Insurance Companies are Starting to Require Cybersecurity—What Do I Do?

(Continued from page 1)

- Web security and firewalls
- Endpoint detection and response (EDR)
- Vulnerability management
- Security awareness training and testing

They might not be especially clear about how to meet these requirements, and they might use some confusing language. Sometimes, the rep you are talking to might not be particularly technical and might have a hard time explaining things beyond the typical script too. We've had clients come to us because they were under the impression that their insurance provider was strictly worried about their website's security, and we've even had clients who strictly follow much more intensive cybersecurity compliance standards who felt that their insurance company was telling them they were missing the mark. To clear these two points up—your insurance company is likely concerned with your all-encompassing IT security:

- **How you collect data** - your website, emails, vendors, internal endpoints, etc.
- **How you store data** - your infrastructure, your hosting, the cloud, your backup, etc.
- **Who you give access to your data** - your staff, your access levels, your vendors, etc.
- **How you are protecting your company** - your security infrastructure, monitoring, security policies, training, etc.

That involves a whole lot of different technologies, so it's easy to get caught up on one particular thing—just keep in mind that it's all-encompassing.
Also keep in mind, your insurance company doesn't know anything about your network or your overall security. They are simply asking you if you have certain safeguards in place or meet certain guidelines. You might have some of their requirements in place, you might not. Some of them will likely just be policy-based, others will require an actual addition or solution.

Your insurance provider will likely tell you that it will keep your policy costs lower to comply, and if you don't, your policy will increase, or they might not...

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

Employee Spotlight: Eric Newhouse

(Continued from page 1)
security and compliance needs of our clientele.

About my role at Indevtech:

As Centralized Services Manager, I oversee Indevtech's suite of backend services and systems that enable us to centrally deliver on our promise of world-class security and productivity at scale across our client base. If I am doing my job right, you won't even know I'm there, but you are reaping the benefits of my work every day through higher performance and efficiency, and reduced cybersecurity risk.

In the past 5 years or so, Centralized Services has become the nerve hub of the security-first MSP, since 90% of our tool stack is now entirely focused on cybersecurity. My role has evolved from monitoring and maintaining systems to being responsible for our entire suite of security products and platforms. Keeping our thousands of endpoints safe and secure 24/7 is our primary goal.

Share this Article!
https://bit.ly/419mK45

Data Can Help Solve a Lot of Your Business' Problems

Today, a business can get more information to help them run successfully than ever before. Unfortunately, a lot of organizations don't use this data to their advantage. Let's go over a few ways that this can be fixed for the betterment of your business' operations.

First, What Qualifies as "Data?"

Generally speaking, the data that businesses collect can be sorted into four different categories. These categories are:

1. **Personal Data** - This category is composed of all the data that can be used to help identify your prospects and clients. This includes both personally identifiable information and details like the devices used, IP addresses, and such.
2. **Engagement Data** - How do your prospects and clients interact with your business and brand? This data helps describe just this, charting the response that your website, social media, advertising, and other efforts to communicate receive.
3. **Behavioral Data** - When your clients, customers, and prospects do interact with your business, how is it that they typically do so? Including datasets like purchase histories and even mouse movements while navigating your website, this form of data seeks to answer this question.
4. **Attitudinal Data -** This form of data helps to measure the response that your business' products and services elicit in your audience. How satisfied are they after completing a transaction? How much interest is there in your product offering?

What Does Data Do for a Business?

There are various ways that the data you collect during your normal operations can be put to use:

Data Gives You Insights into Your Customers and Clients

Today, it is critical that your business has some perspective into how your clientele thinks, what they are most interested in, and what they are really looking for in your business. First of all, who are your clients, and from there, how can you most effectively fulfill their needs and communicate these capabilities with them? Are your current efforts actually returning an acceptable return on your investments? The better you know your audience, the more equipped you will be for success.

Data Helps You Measure Internal Performance

Let's say that Employee A and Employee B spend their time making widgets. By collecting and compiling various data points, you can help determine where your business' internal strengths and weaknesses lie.

Perhaps Employee A's output far outpaces that of Employee B. While this is important data to consider, it can easily tell an incomplete story. Maybe Employee A produces more widgets, but a much higher proportion of theirs don't pass your quality control checks, whereas Employee B's consistently do. Alternatively, Employee A may have logged more training on the widget-making machines, whereas Employee B seems to have specialized more in producing doodads. Having this level of insight into your processes gives you the ammunition needed to make the most of them.

Data Allows You to Finesse Your Processes

On a related note, collecting data throughout your processes can help you to identify points in your business' procedures that can have their costs—both in terms of finances and time—more...

Read the Rest Online!
http://bit.ly/3yCRmOG

You Need to Update Your Continuity Plans

Business continuity is one of those things that can easily be overlooked as most businesses do whatever they can to focus on the job at hand. Unfortunately for the unprepared business, there are a lot of situations that can happen that can interrupt its ability to function optimally. Having continuity strategies in place can save organizations a lot of time and money as they are able to get back up and running effectively quicker.

All this means is that as circumstances change, these plans have to change with them. What if you try to use a continuity plan that doesn't share the reality that your business conducts business in? You will be scurrying around trying to come up with plans on the fly that should have been in place from the beginning. Your margin for error will be smaller, and some businesses won't be able to recover.

There are True Disasters

Take, for instance, the omnipresent threat of natural disasters. Regardless of where your business is located, your business is always at the mercy of nature. Areas that experience harsh winters should be wary of heavy snow and ice accumulation, which can topple power lines and lead to power surges. Some locations are at great risk of tornadoes, which can, quite literally, throw all of your profits into the air. Fires, electrical storms, and other more common natural disasters can all lead to data loss, and there's often nothing you can do to stop it.

You Could Get Hacked

Add in the constant threat of hackers, who are unpredictable and difficult to plan for, and you could have a full-blown data loss disaster on your hands when you least expect it. Unlike a natural disaster, which has telltale signs of impending doom, hackers will brutally assault your business with whatever means they deem necessary to steal or destroy your data. If they succeed, your budget could break under heavy compliance fines associated with sensitive or personal credentials, and your company's reputation could suffer.

Someone Can Just Mess Up

Not to mention that your organization could fall to simple user error. If someone inexperienced or untrained on how to properly handle your data messes with settings or files that they shouldn't be messing with, you could lose track of files, or even risk them to online attacks. This is one reason why it's always important to both educate your employees on best practices, and to use a powerful backup and disaster recovery solution.

What Indevtech suggests implementing is called a backup and disaster recovery (BDR) device, which is designed to minimize downtime when faced with a crippling disaster. BDR is capable of taking multiple backups per day, which can then be stored and recovered from a secure, offsite data center, and the cloud. The BDR can minimize downtime further by temporarily taking the place of...

Read the Rest Online!
http://bit.ly/3ZSjCJa

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
Only 4.5 billion people across the world have a working toilet, but more than 6 billion people have mobile phones.

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