INDEVTECH

TECHMinutes

Your Small Business Technology Information Source!

This Issue:

VoIP is a Great Choice for Businesses

Few parts of your technology infrastructure will have such a profound impact on your operations as your communications systems. Whether it's your email or your phone systems, you're bound to use them on a daily basis, and you'll feel a significant deficit in your operations without them. Today we want to look at one particular solution and ask if it's right for you (hint: it is)...

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

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 Biography: Cheyne Manalo

Last year we welcomed Cheyne Manalo to our team of dedicated technology professionals. Cheyne joins us as Chief Information Officer. Now we'd like to take a moment to introduce you to Cheyne!

Cheyne comes to Indevtech with 18 years of experience in the IT field and has held executive-level positions at many local companies we can all recognize, such as HECO, Foodland Supermarkets, and Aqua-Aston Hospitality.

Cheyne's passion is in team leadership and building effective, scalable processes. At HECO, he managed the IT infrastructure serving over 2,000 critical HECO employees. At Foodland, Cheyne was responsible for building the entire IT department team structure and overseeing digital transformation projects, including developing Foodland's mobile app.

(Continued on page 3)

Mobile Technology Helps You Not Miss a Bit While on the Road

Travel has become pretty commonplace for businesses, and today, business travelers can do more than ever thanks to dynamic mobile computing tools. In this month's newsletter, we will outline some of the most important mobile technologies available to help serve a business while its people are on the move.

Smartphones

The most important piece of technology is one that is also considered problematic by many business leaders. Today, nearly everyone has a smartphone on their person most of the time, and while mobile users can spend a lot of time and effort not doing their work, these tools also provide the best option when it comes to mobile productivity. Not only can you accomplish most correspondence tasks on a smartphone, but you can also do quite a bit with it as a center for other computing.

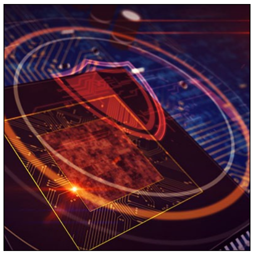
For example, if you are traveling for work and there is a need for one of your traveling employees to complete a crucial task as a part of a project or sale, they can typically use their smartphone as a mobile hotspot in which to connect their computer. The smartphone effectively becomes a modem and router and enables traveling production teams to handle their business without having to connect to any dangerous networks. Of course, this can inject quite a few alternative costs, but if you need to produce on the go, the mobile hotspot through a mobile device can be a great tool.

Virtual Private Network

On the other hand, if mobile data costs are an issue for your business, one of the best ways to ensure that your team isn't putting company data and credentials at risk is to use a Virtual Private Network (VPN). There are definitely different levels of VPN available, and some are more effective at keeping data secure for businesses. These business-specific VPNs can

(Continued on page 2)

Unpacking Zero-Trust's Benefits and If It Is Right For Your Business



When dealing with business computing, there are many situations where threats could potentially ruin the good thing you've got going. Today, a lot of businesses are getting much more serious about their IT security with what is known as a "zero-trust policy". What exactly is a zero-trust policy? This month we will explain it.

Zero-Trust Means Just That

For the most part, businesses that make strides to secure their network and infrastructure have used the same methods for decades. They deploy software to help them secure the network, they manage access and make sure their staff knows how to create secure passwords and identify phishing emails. Zero-Trust doesn't eliminate those, but what it does is take away any space for error. Any device hooked into the network is treated like a stand-alone foreign entity and every user, a foreign user; there is no inherent trust.

What Does Zero-Trust Look Like?

While this seems like a solid practice when it comes to your business' IT security, it just isn't right for some companies. First of all, you have productivity to account for and many workers simply get frustrated when their aim is to do their job, but are interrupted by a lot of hoops to jump through just to gain access. Every business is different and has different needs and some companies simply have far too many moving parts to make a dedicated zero-trust policy work for them.

Consider businesses that have vast computing infrastructures that span several locations. The cost alone to secure so many devices is prohibitive in setting up this policy. So if you are thinking about doing zero-trust security, you may want to implement it on certain systems and not on others. This can lead to convolution, and anyone that knows IT security at all knows that the simpler it is on administrators the more successful it will be. Since businesses might have to acquire new hardware and services, train technicians, and frequently update all of this technology to keep up with security standards, it could just be a lot for an established company.

Despite Those Concerns There Is Immense Security Value

There are significant hurdles involved with zero-trust, but here are five reasons why the strategy does make sense for certain organizations:

- You gain greater control over data means delegation to appropriate users.
- Provides a construct for stronger authentication and authorization policies.
- It can provide a much cleaner user experience (single sign-on).
- Every action and device is subject to policy, leaving nothing to chance.
- Mandates the need for comprehensive access logs.

Build a More Secure Computing Infrastructure

Network security is a big concept and needs big action to do it right. The IT professionals at Indevtech can help you set up your business' IT in a lot of different ways, and zero-trust is one that a lot of businesses are moving toward with the major risks that come with all the cyberthreats out there at this time. Give us a call today at (808) 529-4605 to learn more about how we can help you build a robust and secure computing infrastructure.

Share this Article!
https://bit.ly/3FH8xSd

Mobile Technology Helps You Not Miss a Bit While on the Road

(Continued from page 1)

handle more users and are designed to accommodate the data protection necessary for whole organizations.

The VPN effectively opens up a direct pathway between the business' network and the mobile user, and using encryption, jumbles the data so that if it is somehow intercepted, it is nearly impossible to use. By encrypting all data in transit, you don't have to worry about the extremely insecure connections people usually have to use when they are on the road, or working remotely.

Cloud Services

One of the biggest hurdles to a business' mobility is access—access to the data and software needed to complete its objectives. At least, that used to be the case. Nowadays, cloud services allow effectively any business processes to be carried out from anywhere that a reliable Internet connection can be obtained. Minutely scalable and fully-featured applications, accessible data storage, and more can all be provided to your users through the cloud. Plus, the subscription-based nature of cloud services is simpler to budget for, as costs are made more predictable on a month-to-month basis.

We Can Help You Equip Your Team for Mobility

Find out more about what we can do to support your operations, both in the office and out. Call (808) 529-4605 to talk to one of our professionals.

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

Employee Biography: Cheyne Manalo

(Continued from page 1)

At Aqua-Aston, Cheyne built an in-house team of thirteen IT professionals to manage the company's portfolio of (40) geographically dispersed properties around Hawaii, North and South America.

Cheyne is adamant about personal professional development and has earned (13) certifications, including the coveted ITIL, PMP and CISSP designations, among others.

At Indevtech, Cheyne will head up our new Compliance-as-a-Service initiatives and will oversee proactive services, in alignment with Indevtech's vision to bring Enterprise-class Compliance and Cybersecurity to the SMB market.

Cheyne is truly a "Multiplier" as defined by Liz Wiseman's bestseller Multipliers: How the Best Leaders Make Everyone Smarter and in three short months, Cheyne has already made an already great company even better.

Share this Article!
https://bit.ly/3WFr60i

Could Your Business Resist a Hacker? Here's How to Find Out

Let's say that, right now, someone was attempting to break into your network…could they do it? Is there some vulnerability present on your network that has left you open to attack? This is a question you need to know the answer to so that you can resolve it.

One way to get this answer is by bringing on a professional to perform a penetration test on your business IT.

What is a Penetration Test?

In essence, a penetration test is where you bring on a security professional who simulates a hack as though they were a cybercriminal so that underlying and unnoticed vulnerabilities can be identified and resolved. Your IT network is a complicated maze of interconnected pieces of hardware and software titles…any of which could very well have vulnerabilities hiding in them. All a hacker needs to do is find one of these vulnerabilities, and you're in for a very bad time.

As they perform a penetration test, the security professional will go about the task of hacking into your network exactly as a cybercriminal would. This is what is known as "ethical hacking," and is done so that you can resolve the aforementioned vulnerabilities in your network. This is an important step in preventing data breaches, which is the ideal outcome. It is always better to avoid a security incident than it is to recover from one, which is what makes preventative action so critical.

Penetration Testing Does More Than Just Find Weak Points, Too

While the primary goal of a penetration test is to identify a network's vulnerabilities, it can also provide other insights as well. For example, a penetration test also applies pressure to your systems, which allows you to see how your infrastructure responds.

Generally speaking, there are three different types of penetration tests:

- When **black box testing,** the person administering the penetration test goes in with no knowledge of the network or what data they should target. This kind of test might be used as a diagnostic if there are no specific issues being sought out.
- **White box testing** is the opposite scenario, where the tester goes in with prior knowledge of the network makeup and the specific issues that are being evaluated and resolved.
- **Gray box testing** is a mix of the two, where the person running the test has some partial knowledge of the network they are trying to breach.

The results of the evaluation are then compiled into a report that details what the tester was able to accomplish, like how far in they managed to get and what data they managed to "steal." This informs the business about what needs to be fixed so they can, well, fix it, before a real attack comes along and uses the vulnerabilities to its advantage.

Don't Leave Yourself in the Dark in Regard to Your Security!

With the challenge that cybersecurity can pose for small businesses and their relatively limited resources, you could probably use all the help you can get. Indevtech is here to provide that help through our comprehensive IT solutions and services, including cybersecurity. Our goal is to make your business as secure and efficient as possible, in large part by developing a robust cybersecurity strategy. A penetration test helps us do that.

Find out more about our services and how they can benefit you by calling (808) 529-4605.

Share this Article!
https://bit.ly/3Wleew3

Cybersecurity Needs to Be a Part of Your 2023 IT Strategy

In today's digital world, SMBs need to establish a comprehensive cybersecurity strategy to protect themselves from a range of potential threats. Whether it's a small business with a handful of employees or a large corporation with thousands of workers, every organization is vulnerable to cyberattacks. That's worth stressing because so many business owners think they are immune simply because of the size of their organization.

One of the key considerations for any cybersecurity strategy is to recognize that no system is ever 100 percent secure. Hackers are constantly developing new ways to breach even the most well-defended systems, so it's important for businesses to be proactive in their approach to cybersecurity. This means regularly updating and patching software, implementing strong passwords and authentication protocols, and training employees on best practices for security.

In addition to the technical aspects of cybersecurity, businesses also need to consider the human element. Employees can be a major weak point in any organization's defenses, so it's important to educate them about the risks of phishing attacks, malware, and other common threats. This might include regular training sessions, as well as implementing strict policies around password management and the use of personal devices for work.

The Costs of Ignoring the Problem

Another important consideration for businesses is the financial impact of a cyberattack. The costs associated with a breach can be significant, including the loss of sensitive data, damage to the company's reputation, downtime and lack of productivity, and potential legal action. As such, it's essential for businesses to have a plan in place to respond to a cyberattack and minimize the potential damage. This might include working with an IT company like Indevtech to quickly identify and address the breach, as well as having insurance in place to cover the costs of recovery.

Let's take a look at the most common type of attack, ransomware.

Ransomware is a type of cyberthreat that has become increasingly common in recent years. This malicious software encrypts a victim's files and demands payment in exchange for the decryption key, which can be a major inconvenience for businesses of all sizes. However, for small businesses, the financial impact of a ransomware attack can be particularly severe.

One of the most obvious costs associated with ransomware is the ransom itself. Ransom amounts can vary, but they are often in the thousands of dollars. For a small business with limited resources, paying that ransom seems like the easy way to get out of trouble, but we advise **not paying the ransom**. That only incentivizes the criminals, and there is no guarantee that it will actually get your data back. Remember, you are dealing with criminals.

Then there is lost productivity. When a business' files are encrypted by ransomware, employees may not be able to access important documents and systems, which can prevent them from being able…

Read the Rest Online!
https://bit.ly/3W5wCJv

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
The digital universe contains over 44 zettabytes of data.

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