Excalibur TECHNOLOGY
www.excaltech.com • [877] NET - KING

TECHBytes
September 2017

"When it HAS to work, call Excalibur Technology!"

In This Issue:

What Should You Know About Regulatory Compliance?

3 Ways Managed IT Creates Benefits for Your Business

Will These End Of Life Events Affect Your Company's IT?

Comparing Cost and Control Between In-House Architectures and Cloud

What Plans Does Your Organization Have for Communications?

Security Terms That Every User Needs To Know

Will These End Of Life Events Affect Your Company's IT?

One of the best ways your organization's network can remain secure is to always use the most recent version of any critical software solutions on your network. Unfortunately, making the jump to a more recent operating system is easier said than done, particularly for small...

Read the Rest Online!
http://bit.ly/2xgwxuu

About Excalibur Technology Corp.

Business owners demand simple, reliable and powerful technology solutions to keep them ahead of their competition while reducing their costs; solutions that require expertise, teamwork and dedication. Excalibur Technology has built a reputation for excelling at helping our business clients achieve these goals.

Visit us **online** at:
www.excaltech.com

What Should You Know About Regulatory Compliance?

When you sit down with new prospects, you rarely talk about data security. The client is usually focused on the problem they have that has made them come to you in the first place, while you are likely focused on closing in on bringing critical revenue into your business. That doesn't mean that data security isn't an extremely big issue, it just that without business, it is a non-issue.

With electronic record keeping at an all-time high, and the number of miscreants out there looking to gain access to those files, certain industries have outlined a series of regulations that businesses that work with potentially sensitive data have to adhere to. Industries like health and finance have the most strident regulations, as governments begin to set legal ground rules for the reporting and security of critical data.

To ensure that your company meets any compliance standards to which it is mandated, Excalibur Technology is versed in the technical aspects of data protection and can help you remain compliant with your industry's regulations.

Government Mandates: In certain industries, normally ones where the data is the most lucrative, state and federal governments create regulations that organizations need to meet. Typically, these compliance standards are issued with attention on network and data security, and the protection of the dissemination of the data. The cost of keeping networks and data secure, reporting for transparency, and any noncompliance costs are absorbed by the organization, making it extremely important to adhere to and maintain regulatory compliance.

- HIPAA is required by the Office of Health and Human Services (U.S. Government).
- SOX is required by all publicly held companies.

(Continued on page 2)

3 Ways Managed IT Creates Benefits For Your Business

Does your business technology help you improve operations, or does it hinder your staff to the point where it's nothing but a frustration? Chances are that your business requires considerable IT maintenance just to keep things moving forward, but if yourself and your employees are responsible for such a duty, you could be wasting valuable time and effort for other business ventures. To solve this dilemma, you should consider managed IT services for your network maintenance.

Here are three ways that managed IT beats out the competition in terms of providing your organization the best service possible at the best rate.

Managed IT is Less Expensive

If you have an internal IT department that keeps issues to a minimum, you're one of the lucky small businesses with budgets flexible enough to handle the investment. The truth is that it's not easy to hire an entire internal team dedicated to keeping your organization up and running; and, most SMBs struggle with such an expense. Managed IT is an outsourced solution that allows you to prevent issues from popping up in the first place, and

(Continued on page 3)

What Should You Know About Regulatory Compliance?

(Continued from page 1)

- New York State requires all financial organization to meet Cyber Security Requirements for Financial Services Companies.

Internal Mandates: Since many businesses that have had to deal with the fallout of significant data breaches come out significantly less prosperous, many organizations have begun to be more diligent about the way they share and store potentially sensitive data. Some internal regulations include:

- Bring Your Own Device (BYOD) policies do a thorough job of controlling what devices have access to your organization's network.
- Remote Access is helping all types of organization be more productive. Companies that to allow for remote access often lean on a Virtual Private Network (VPN) to ensure that when a member of your team needs access, that they have it through secure means.

Continuity Policies: Most of the regulations set forth by the government require some degree of continuity planning. This includes a reliable backup and recovery solution as well as a more detailed and robust disaster recovery strategy. Since managed service providers are in a position to help secure data, manage and maintain hardware, and thoroughly inventory all hardware and software assets an organization holds, they are the ideal partner to help outline your continuity policy.

Vulnerability Assessment: The more secure your organization's network is, the better. To help ascertain just how secure a network is, a penetration test is mandated by regulatory bodies. Basically, the penetration test is a deliberate attack on an organization's network by a friendly party. Vulnerability assessments are often required, as well. A vulnerability assessment is a report that indicates where there are weak spots in a network. Along with performing these tasks, an MSP can also provide the necessary paperwork required to prove security measures are being taken.

Remote Monitoring and Maintenance: Keeping an artful watch over your network can be one way to keep nefarious and unwanted entities out of your network. Typically, any compliance mandate requires an organization to have some semblance of monitoring in place as a protection. MSPs have certified technicians on staff whose job is to monitor and manage client networks, improving the network coverage.

No matter what you are required to report, or your organizational technology needs, Excalibur Technology has the experience and knowledge to help you protect your business. For more information about network security, call us today at (877) NET - KING.

Share this Article!
http://bit.ly/2w6R9Br

Comparing Cost And Control Between In-House Architectures And Cloud

The benefits of the cloud are almost too numerable to count, but you shouldn't let this dissuade you from other possibilities. After all, what works for one business may not work for another. For organizations that don't find the cloud to be the best method of data distribution, an in-house infrastructure is absolutely critical. How can you determine which of these solutions is ideal for your business?

Let's take a look at two features that will be a major deciding factor for your infrastructure design: cost and control.

Cost

Capital is one of the most crucial parts of any business. After all, it's your goal to make money from your organization, so you want to make sure that you're able to comfortably afford your operational equipment. An outsourced cloud provider has an advantage over an in-house infrastructure in regard to the cost of maintenance. Financially, it takes a considerable amount of capital to maintain your infrastructure, especially if it's located in-house. Your in-house technology infrastructure contains expensive technology, and it only grows more expensive when you have to power it and maintain it as well.

An outsourced provider will only provide a flat monthly rate designed around a service level agreement, which makes it easy to place into your budget. Operating a server in-house can be a bigger investment, so choosing to outsource gives your organization the opportunity to dedicate those resources to something else.

Control

It's natural to want control over your infrastructure. Unfortunately, this desire for control can keep you from investing in a solution like outsourced cloud hosting, even if it is beneficial for your organization. If you are worried about having full control over your business's infrastructure, perhaps it would be easier on your nerves and your management style to focus on your in-house network. However, outsourcing can be just as relieving, as it removes the responsibility of managing your technology completely, freeing up even more time and resources for other uses. It basically comes down to how much you trust either your in-house team or your managed service provider.

The Ideal Solution

Regardless of your company's needs, Excalibur Technology is here to help you ensure that your network…

Read the Rest Online!
http://bit.ly/2hhJ5I0

3 Ways Managed IT Creates Benefits For Your Business

(Continued from page 1)

resolving them before they are impossible to contain. Since you're only paying for a monthly fee rather than multiple annual salaries, you'll wind up saving money in the long run.

Managed IT Doesn't Require Your Attention

Managed IT doesn't interrupt your operations when an issue becomes apparent. Instead, the issue could possibly be resolved without you even knowing that it had existed. Remote monitoring and maintenance allows a managed IT provider to keep watch for these issues, and if it's covered under your service level agreement, we'll fix it before it interrupts the way your business functions.

We'll always notify you if something requires your attention, but most problems can be resolved without an on-site visit. This cuts down on travel time and downtime, since you won't have to wait for a technician to arrive on-site to fix the issue.

Managed IT is More Flexible

Managed IT services offer so many solutions that you can achieve just about all of your needs through a specific service plan from Excalibur Technology. If you only need basic solutions like implementation of an email application, or you need your entire infrastructure managed and maintained, we can help your organization ensure optimal operations. It's all about your business's IT, and we'll do what we can to keep your technology working as intended, if not even better than before.

You don't have time to manage its own IT, and you shouldn't need to. Your primary goal should be to keep your focus on managing your business, not your technology. That's why Excalibur Technology is here, after all.

We want you to devote your attention to running your business and creating more lucrative opportunities. You can count on us to be there to keep your mission-critical technology running as intended. To learn more, reach out to us at (877) NET - KING.

Share this Article!
http://bit.ly/2xi6d0k

What Plans Does Your Organization Have For Communications?

Over the past few decades, technology has drastically changed the way businesses of all sizes and industries communicate. In fact, there is a direct correlation between the way a business communicates and its overall success. The majority of customers, as well as their employees, demand that the modern business find avenues of sharing information that are as close to instantaneous as possible.

To meet this demand, the future of business communication strategy will likely utilize multiple platforms, including email, phone, instant messaging and social media. For many businesses, the future has arrived - at least partially. Multiple avenues of communication are already being adopted by many companies, to great success. Have you given any thought as to whether you're giving your business the opportunity to drive service and productivity through the best type of interaction?

Email

Once dominated by telephone usage, email is the predominant method of business-related correspondence. It's inexpensive and efficient and can be accessed easily from practically anywhere. Email can be secured through encryption, as well as used retained and stored as a documented record of an exchange.

By the Numbers:

- 93% say they're likely to respond to email.
- 94% recommend people contact them by email.
- 86% say they use email daily.

Phone

The telephone may have been invented a hundred years ago, but it's still one of the most popular ways to reach another person and interact in real time. While telephone communication through digital and cellular services steadily climbing, the use of landlines, or phones that require a connection to traditional, copper wires to operate, are rapidly declining.

Internet-based telephone platforms, such as Voice over Internet Protocol. (VoIP), are ideal for businesses because its capabilities dwarf that of landlines. VoIP gives users the option of have their phone ring at multiple locations (ex. desk, smartphone and home) simultaneously or in a cascade. It reduces the amount of hardware required and is less expensive than other phone options.

By the Numbers:

- Only 54% use their landline on a daily basis
- 76% recommended reaching out to them by cell phone.
- 78% are likely to respond to a voicemail.

Chat Interface

Particularly popular with internal communications, instant messaging (IMs) allows users to chat in real time, and well as while carrying-on multiple discussions with several team members. Similar to email, it is possible to…

Read the Rest Online!
http://bit.ly/2xfR0j3

Security Terms That Every User Needs To Know

Chances are that you've seen quite a lot of stories on the Internet, or in the news, about the many security threats out there. Some of these, including ransomware, exploits, and reluctance to update software, might fly over your head if they're not part of your everyday business vocabulary. Knowing what these terms mean is of the utmost importance in today's workplace. We're here to help you understand what some of these security terms mean for your organization.

Ransomware like WannaCry are one of the primary reasons why it's so important to understand how network security works, and all of the terminology behind it. After all, hackers understand how to exploit your network's weaknesses, so you'll want to know all about the primary way to protect your business's data from them: security patches.

These patches are issued by software developers to resolve certain issues or troubles found in their products. For example, a patch might be designed to address a recently found vulnerability in the program's code, or resolve a particularly troublesome issue with the user interface. Understanding how these patches work is critical if you want to ensure the security of your business, your personal computer, and everything in between. Here are five of the most common terms used when speaking of security patches.

Patch Tuesday

Even if you allow your computers to update and install patches automatically, you should still have an idea when these patches are installed. Microsoft has a set schedule that they use to release these patches. They are released on specific days of the week, including the second Tuesday of each month, and sometimes the fourth as well. Perhaps in the future, data exchange will allow newer operating systems to be updated more frequently, or at the very least in real time, keeping your systems more secure.

Security Patching

Patches are basically issued to fix something that's wrong with a computer application or program. It is these patches and updates that are provided on all of the official patch days, like Patch Tuesday. Of course, immediate patches to imminent threats of Microsoft's software are issued for release as soon as one is created. These zero-day threats are so dangerous that they need to be resolved as soon as possible, making them top-priority for your organization.

Hotfixes

These are sometimes called quick fix updates, quick-fix engineering updates, and general distribution releases. These hotfixes generally include a patch that fixes just one small thing wrong with your application. These small issues are usually important enough that they need to be issued immediately without waiting for the next batch of patches. Even though Microsoft has long since forsaken the term "hotfix" specifically, it's still used as a common way to refer to these fixes in the technology sector.

Zero-Day Threats

These types of weaknesses are those that are being used by hackers even before they are discovered by security professionals. The name "zero-day" refers to the fact that the software developers have no time, or zero days, to develop a patch to resolve the issue. These are some of the most dangerous threats out there, and need to be a...

Read the Rest Online!
http://bit.ly/2fAnwlN

CHROME MAY SHOW YOUR SITE AS "NOT SECURE"!

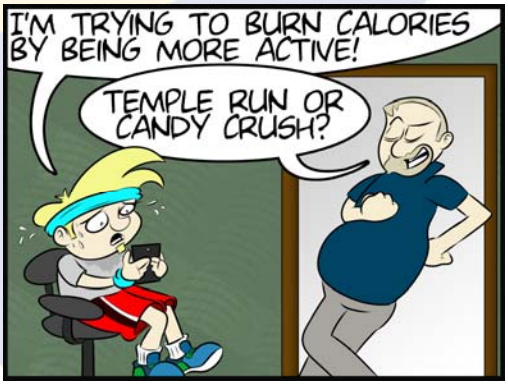
If your website is not secured with an SSL certificate (HTTPS), Google Chrome will soon display a "Not secure" warning when users type into any form on your site. This includes contact forms, login forms, and even simple search boxes.

Don't let this happen to your website. Call us today to have our experts configure your site to load securely and avoid this warning!

Read the Rest Online!
http://bit.ly/2xiyeam

Tech Trivia

Using your phone while it is on charge can damage the battery, this is why the leads for the chargers are so short.



Excalibur Technology Corp.

Barrington, IL
Clearwater, FL

Toll-Free: 877-NET-KING

Visit us **online** at:
www.excaltech.com

facebook.excaltech.com
linkedin.excaltech.com
twitter.excaltech.com
blog.excaltech.com
support@excaltech.com