Total Networks
Business IT Done Right

NetworkNews
September 2017

This Issue:

Why SaaS Is Best For Your Business' Software Needs

All businesses have certain software solutions that they need to keep their operations going. Be it an email solution or a productivity suite that you lack, your business is held back from...

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

About Total Networks

Locally owned and operated since 1986, Total Networks is the only firm in Arizona to receive CompTIA's Security Trustmark validating the firm's adherence to best practices for information security. Services include IT support, security & compliance assessments, document management, backup & disaster recovery and IT planning/CIO services.

Visit us **online** at:
totalnetworks.com

You're Invited: Total Networks Open House

For the past few months, we've featured articles in our newsletter about our office expansion and the new members of the Total Networks team. As your IT partner, we feel it's important to put faces to the names that we serve. We want you to be able to do the same.

We'd like to invite you to our Open House event where you'll be able to meet everyone from our management, technical and administrative teams – yes, even Debbie will be here – and see our newly expanded office space.

Date: September 21, 2017
Time: 4:30 pm – 7:00 pm
Location: Arizona State Bar Building, 4201 N 24th Street, Suite 230
♦Appetizers & Beverages will be served
Please contact:
amarshall@totalnetworks.com **by September 17th to RSVP**

We look forward to seeing you there!

Teaching Leadership & Strength Through Surfing

For two weeks every summer our Technical Team Leader, Paul Miller, heads off to San Diego, California to help lead a youth surf camp – the Lucky Sevan Grommets Surf School Expedition.

Lucky Sevan was founded by Evan Rogers and Todd Skinner, both of Skinner + Company, and Paul Miller in 2006. The surf school is a way to help young men overcome and face life challenges and view them instead as opportunities for growth. This year's surf expedition was held in July. When they arrive at camp, each participant is assigned to a team that is led by adult mentors. In addition to learning how to surf, they participate in games, drills and devotionals to learn qualities that are essential to teamwork, leadership and service to others. In addition to the week-long camp for young men, in 2013 the program added another week in order to host a surf camp for young women Lucky Sevan Wahines.

If you are interested in learning more about the program or donating, please contact Evan Rogers at (602) 620-3417 for more information.

Share this Article!
http://bit.ly/2wgcb3r

What Makes Managed IT the Best Option?

Who would you rather hire–an employee who comes in late, after your systems have encountered an issue, and takes twice as long to fix them as he said, or an employee who was ahead of the game, and managed to avoid issues before they influenced your business? This scenario is precisely the same one that you encounter when you weigh a break/fix IT provider against a managed service provider.

In order to understand the differences between the break/fix and managed services approaches, it may be helpful to run

(Continued on page 3)

What Hackers Are Looking For On Your Network

When a hacker tries to infiltrate your network, they are doing so with a purpose in mind. Usually they are looking for specific information, like account credentials, personal information, or files that can be used to blackmail victims. Regardless, we'll go over what a hacker can do with the information that they collect from you, and how you can best protect it from them.

The Information Itself

All businesses hold some sensitive information that hackers will do anything it takes to get their hands on. For example, consider what kind of information is collected by the typical business' human resources department. Naturally, they need all of their employees' information on record, including birth dates, Social Security numbers, contact information, and other sensitive information. Other departments, like accounting, might need access to financial credentials like credit card numbers or bank account numbers. All of this information is quite valuable for hackers, and they do what they must in order to try and steal it.

Other times, hackers will just try to plant malware – like a keylogger or ransomware, on your company's network to collect or steal information, like usernames, passwords, and other account credentials. They may then try to use these credentials to hijack accounts or access further information related to your organization, which could result in a major data breach that threatens both the reputation and future of your business.

Sometimes hackers aren't after information at all, and would rather just cause trouble. Other times, they might plant something like a trojan to create a backdoor for later access. Regardless, hackers are looking to take advantage of your organization's assets in ways which should cause concern.

The Solution

A comprehensive security solution such as a Unified Threat Management (UTM) solution is your best chance to defend sensitive information from prying eyes. A UTM combines some of the best...

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

3 Trends That Are Changing the Role IT Plays for Your Business

Your IT is a central part of your organization's operations, but its role has changed significantly as business processes have grown more streamlined. There are always shifts and changes in the way that businesses function which must be accounted for, especially in the modern office environment. How have these shifts affected your business's IT management?

We'll discuss three of the most important new trends that your organization likely has to deal with, especially if you want to ensure the continued security of your organization's technology and data.

Increase in Mobility

The use of mobile devices is a major trend that is helping employees be more productive, but at the cost of network security. While solutions like the cloud are allowing employees to access data and applications on their mobile devices, this prompts them to bring the devices both into the office and on the road with them. This type of mobility could create a situation where your data is put at risk, even if it's through no fault of the employee themselves.

To counter this notion, businesses have begun to implement Bring Your Own Device (BYOD) policies that reinforce proper security practices on mobile devices. This includes everything from mobile wiping of devices to whitelisting apps that are needed and blacklisting apps that are wasteful or dangerous. The idea is to educate your employees on proper security practices, and reinforcing these practices with technology solutions to shore up any notable weaknesses.

A Focus on Security

Security has always been important for businesses, but now it's more so than just about anything else. The threat landscape has considerably changed over the past decade. While the most dangerous threat out there consisted of viruses or malware that could halt your operations or steal data, there are even greater threats out there that have increased the level of security required in order to preserve your business.

Advanced phishing attacks that impersonate higher-ups in your organization pose a greater threat than before. Furthermore, ransomware has become a major part of any would-be hacker's toolkit, extorting funds from unfortunate victims to further their hacking campaigns. Only the best enterprise security tools and knowledge of these advanced threats can be enough to keep them at bay.

From Reactive to Proactive

In the past, businesses would focus on alleviating problems as they crop up. The belief was that they would save money by only administering maintenance when it was really necessary, rather than trying to spend money when it wasn't. Unfortunately, this...

Read this Rest Online!
http://bit.ly/2wgoop1

What Makes Managed IT the Best Option?

(Continued from page 1)
through how a common issue as it would be handled by each.

Break/Fix

As its name would suggest, the break/fix approach comes into play when some component of your IT breaks, and someone has to come in-house to fix it. While this approach was effective enough for a few years, it is no longer the best option to consider for your business and its needs.

This is largely based on the speed that business moves at today, with the help of technology. Imagine this situation happening to you: a piece of your hardware goes on the fritz. Of course, this hardware was necessary for a few of your employees to be productive, so that's revenue thrown right out the window.

You also have to factor in the price the break/fix repairman plans to charge for their trouble to travel to the office, in addition to the cost of any repairs they make while they're there. If they can't make the repairs with what they have, you're going to have to wait until they have what they need. This also can have the potential for a significant service charge.

So, tallying up so far, break/fix ultimately costs you time and money, in addition to the losses your business will incur because it was at least partially incapacitated for a time. You will also have to pay your staff for the time they spent at work, whether or not they generated any revenue for your company.

Clearly, considering its obvious faults, break/fix simply isn't an economical choice. Fortunately, we still have managed services to examine.

Managed Services

Unlike break/fix, the meaning behind managed services takes a little bit of backstory. Essentially, rather than waiting for an issue to give your systems trouble, a managed service provider will monitor the technology you have in place to keep an eye out for issues, proactively resolving them before they cause operational deficits. For a predictable monthly rate, your managed service provider will handle all of your issues remotely, preventing any issues they can from taking root, and working to fix those that they can't.

This brings the usual tally for a managed service provider's work to be whatever they charge as their monthly fee, with the odd exception of specialty services or work that lies outside of the contract. Even so, managed services allow you to preserve your precious uptime for as long as possible, which is beneficial for your business.

If you're ready to make the switch to managed services, or to hear about our other solutions, give Total Networks a call at (602)412-5025.

Share this Article!
http://bit.ly/2wg0QR2

Tips on Business Continuity Planning from Financial Institutions

Few organizations take business continuity planning as serious as financial organizations do. The Federal Reserve Bank (FRB) and Securities and Exchange Commission (SEC), as well as the organizations they oversee, depend heavily on technology for their daily operations. For these establishments, a severe data loss event or significant downtime has the potential to cripple the economy, depending on the severity. As such, they require all of the institutions that they have jurisdiction over to meet certain business continuity benchmarks.

Even if your companies are not legally required to comply with these regulations, using them as a guideline for your own business continuity plan (BCP) is a great way to ensure that you're prepared for a 'worst-case-scenario'. Here's a look at a few of the elements that the FRB and SEC require for business continuity plans:

Personnel: Human resources represent one of most critical BCP components, and often, personnel issues are not fully integrated into the enterprise-wide plan.

- Team in Charge of BCP
- Define Key Personnel
- Establish Emergency Contacts

Communication Planning: Communication is a critical aspect of a BCP and should include communication with employees, emergency personnel, regulators, vendors/suppliers, customers, etc.

- Notify team of Disaster/Event
- Set-up Information Hotline for Employee Updates
- Keep Updated Phone Tree
- Backup Communication Methods
- Contact Vendors/Customers

Technology Issues: Just as they do during the course of normal business operations, technology issues play a crucial role in the recovery process.

- Define Data Recovery Process
- Employ Multiple Data Backup Storage Locations
- Keep Prioritized Inventory of Technology
- Hardware – mainframe, mid-range, servers, network, end-user;
- Software – applications, operating systems, utilities...

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

What We Can Learn From IT Statistics

Technology plays a pivotal role in the way modern businesses function, and as a result it carries some element of risk. An example of this is how companies store electronic records. While the implementation of measures that are designed to provide greater ease of use and organization for a business' employees make business move faster, it also makes it that much easier for a hacker to locate and steal data. Small and medium-sized businesses, in particular, are vulnerable, as they may not have dedicated IT security.

To give you an idea of how you should approach IT security for your small business, take a look at the following statistics gathered by Netwrix.

- **Only 36 percent of organizations report being fully aware of employee activity on their network.** Are you aware of all activity that happens on your network? It doesn't matter if it's your employees accessing social media, or a former employee accessing their account for who knows what purpose. Only about one-third of companies understand what happens on their network, and ignoring these facts can be a considerable threat to your organization's computing platforms. The more you know about how your network is being used (and by whom), the more you can protect it.
- **The percentage of businesses that have at least some control over employee activity on their network grew from 62 percent in 2016 to 85 percent in 2017.** IT risk reports also contain some positive information. In this case, it's that more employers are noticing the need for IT security. Most security issues happen, in at least some capacity, due to human error by employee behavior on your network. Whether or not they are deliberately trying to sabotage your computing systems is an entirely different story. Regardless, remaining cognizant of the threat to your network is key, so keep track of who accesses what information, and for what reasons.
- **65 percent of respondents admitted to having security incidents in 2016; the most common reasons cited were malware and human errors.** You might be surprised by how often SMBs are targeted by hackers and cyber criminals. The point stands that small businesses that fail to implement safeguards against common security threats can fall victim to data breaches and other attacks.
- **48 percent of organizations that have to comply with any cyber security standard still struggle to ensure continuous compliance and provide complete evidence of it to auditors.** Depending on the industry, some SMBs will have to adhere to specific standards put into place to ensure accountability, among other things. More than this, though, is that auditors require proof that these organizations are adhering to their regulations. This can include anything from policy implementation to compliance audits. It's recommended that you reach out to Total Networks for assistance with ensuring compliance with these often-complicated requirements.
- **79 percent of respondents say that detecting and mitigating human errors, both malicious or accidental is critical for reducing IT risks.** Humans are known to make mistakes. If an employee clicks on the wrong link or downloads the wrong attachment, they could expose your network to all manners of threats. Therefore, risk...

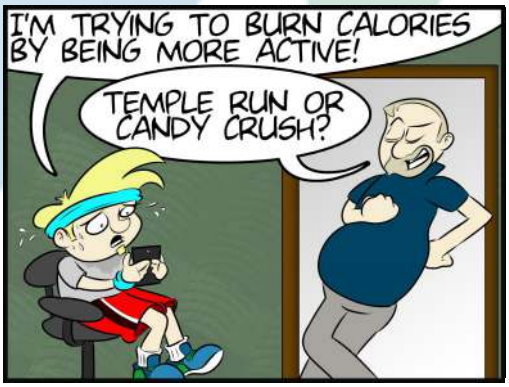
Read the Rest Online!
http://bit.ly/2wjpqR9

We work together with our IT Managed Services clients to jointly create and maintain an up-to-date, effective written technology plan and budget.

If you would like to receive an electronic version of our newsletter please email skinsey@totalnetworks.com

Dave and Stephanie Kinsey
Owners

Bo Brown
Business Development Manager



Total Networks

4201 North 24th Street
Suite 230
Phoenix, AZ 85016
Voice: 602-412-5025

Visit us **online** at:
totalnetworks.com

CELEBRATING 30 YEARS ANNIVERSARY

info@totalnetworks.com
facebook.totalnetworks.com
linkedin.totalnetworks.com
twitter.totalnetworks.com