Total Networks
Business IT Done Right

NetworkNews
June 2015

This Issue:

How to Set Up a Business Succession Plan

If something debilitating were to happen to you, could your business carry on? This isn't a pleasant scenario to think about, but it's absolutely necessary to have a contingency plan in place for reasons like this. Also known as a business succession plan, if you have a plan in place, then you don't have to worry about what the future holds, at least, for your business.

Read the Rest Online!
http://bit.ly/1H7rYw6

About Total Networks

Building on the tradition of providing industry best solutions, the Kinseys continue to invest in tools, training, recruiting, and procedures, continuing to extend our reputation as the premier IT service provider in Arizona.

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

Keep Shadow IT from Killing Your Business

Data sprawl is bad enough. Having users decide on their own to implement IT solutions can kill a business.

Shadow IT

Shadow IT is when employees bypass business processes and policies and use unsecure and unmanaged consumer-grade IT solutions for corporate data. Users set up their own free online sharing, remote access, smartphone backups, wireless access points, thumb drives, and other unauthorized risks that they thought were just making their lives easier. They may need access to their data from home or while traveling and don't realize that they are creating security and compliance risks for their firm. Shadow IT is mostly adopted by good people with good intentions, but in some cases it is used maliciously to steal proprietary data.

Too Easy

It is now so easy and inexpensive – often free – for someone to bypass company IT policies and procedures. Users view data casually, not as a valuable business asset or something that if lost can result in an expensive and embarrassing data breach. They treat company files the same as their family pictures, and don't give their managers a vote in where the firm's data ends up.

File Sharing & Backup

File sharing services are good solution but aren't all the same when it comes to securing data, tracking access and offering management a view of what is happening with the data. The firm should be part of any decision if an employee wants to use it to share business info or client files. Free thumb drives given out at conferences can move data from secure networks to a

(Continued on page 2)

Some Hackers Are Out to Give IT Departments a Bad Reputation

We all know that hacking is one of the biggest risks we must deal with in today's technology-based society. Most hackers out there try to take advantage of the latest vulnerabilities in software, but there are some that use a more sophisticated method. These hackers try take advantage of the weaknesses found in the human psyche, rather than the technological flaws that consistently get patched.

Attacks like these are generally classified as phishing scams, in which the hacker will attempt to steal sensitive information by taking advantage of employees who might not know any better. They will often pose as important individuals from recognized institutions, like banks or business partners, and attempt to coerce credentials from your team. These can come through phone calls, emails, or other mediums.

Some of the most offensive crimes against the general populace and this technological society in general are how hackers will often impersonate IT staff to further their own goals. As IT technicians ourselves, this makes us sick. We can't think of a more grievous way to infiltrate a system. Not only do these hackers access systems without permission, but they also ruin the

(Continued on page 3)

Keep Shadow IT from Killing Your Business

(Continued from page 1)

very high risk of loss. Cloud services that make it easy to back up laptops, phones and tablets, may also result in corporate data moving into a location the company doesn't know about.

Email

Data sent to free email services like Gmail, Hotmail, Yahoo!, and those that come with an Internet service can end up anywhere, and cannot be retrieved. Even deleting these may not completely erase them from the vendor's servers and backups.

Who ever thought…?

Uneducated users and wannabe IT "experts" can create real dangers. What if an employee exported the firm's confidential client files onto an insecure device? Could your staff make copies without your knowledge? Once in a secure document management system that met the firm's security standards, the files now can be read by anyone with a computer, there is no tracking of access, and no way to know how many copies are floating around. Considering the high costs of data breaches (both to reputation and notification regulations), this could kill the firm if the data was breached.

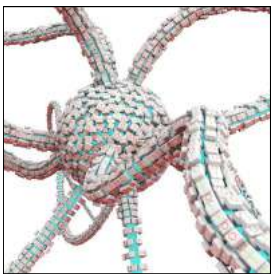
What can managers do?

1. Educate yourself about the pitfalls of having client data stored on devices and locations without your permission.
2. Identify reliable choices of safe solutions to solve your data access problems.
3. Check systems for unauthorized file sharing and data backup software.
4. Implement data loss prevention software to restrict how data can be moved.
5. Establish policies to prohibit unauthorized solutions.
6. Conduct cybersecurity training for your staff.

The more people understand the value of data and the risks of unauthorized data management solutions, the more you will be able to keep IT out of the shadows.

Share This Article!
http://bit.ly/1FD1xli

Using Big Data Gives You a Big Competitive Advantage



Today's technology has accomplished a ton of fascinating things, but none are more important for the average business than big data analytics. When considering the incredibly competitive nature of the business environment, anything that gives your company an edge is a welcome addition to your strategy, and it's more important than ever before to heed this call to action.

What is Big Data?

Big data is the act of analyzing chunks of raw data for trends and other important information. This helps businesses make informed decisions concerning new policies, their target audience, and much, much more. With the knowledge of these trends, your team can apply them to your business model and potentially surpass your competitors.

One example of big data would be a consumer-based company monitoring their social media pages for trends in their followers. They look for patterns in the interests of their followers, including age, gender, liked pages, and more. These trends allow the company to tailor their marketing campaigns to meet the interests of their primary consumer base.

As explained by Bill Detwiler of ZDNet:

"According to a 2014 study by Accenture and General Electric, 84% of the companies surveyed believe that big data analytics could "shift the competitive landscape" for their industry within the next year and 89% believe companies that fail to adopt a big data analytics strategy could lose both market share and momentum."

If what this survey says is correct, businesses who have taken the initiative that big data has to offer will have an incredible advantage over those that don't. Additionally, big data analytic tools are growing more popular and more affordable, making them more readily available to the average small or medium-sized business.

How to Get Started

Unless you have a solid plan for gathering all of the data required for these kinds of analytics, you'll probably run into some trouble at first. Instead of jumping the gun and getting ahead of yourself, consider what kind of data needs to be acquired. According to Max Shron, a data scientist at Polynumeral, it's important to find out what kind of data you need before collecting it. Otherwise, you might collect data that isn't of any use, and you'll have wasted time.

Instead, ask yourself what kind of data your business already possesses. From there, consider what kind of data you need. Once you understand your target, you can go about collecting this data in an organized manner. It's important to put aside any predispositions you might have concerning your data or product. After all, numbers don't lie, and it's much easier to put together a solid plan based on facts rather than remain biased toward your services...

Read the Rest Online!
http://bit.ly/1H7qrWV

Some Hackers Are Out to Give IT Departments a Bad Reputation

(Continued from page 1)

good name of hard-working IT professionals whose goal is to put a stop to attacks like these in the first place.

In fact, the security experts at FireEye have reported that these impersonation crimes rank as some of the most commonly used tactics by hackers. The primary reason these tactics work is due to a lack of two-factor authentication.

As ZDNet reports:

"Social engineering, phishing campaigns and the impersonation of legitimate IT personnel are also on the rise. The security firm says that through 2014, FireEye observed hackers impersonating IT staff in 78 percent of phishing schemes directed at companies, in comparison to just 44 percent in the previous year."

As IT professionals and human beings, we cannot stand idly by while innocent people are targeted. The small or medium-sized business may not have the in-house IT department to constantly keep watch over your company's network. This is why Total Networks offers security solutions that are designed for integration into any network. Our Unified Threat Management (UTM) device is a comprehensive network security measure that includes a firewall, antivirus, spam-blocking, and content-filtering solution, all designed to help your organization cope with the constantly-evolving threat landscape that comes with the business environment.

"Don't let hackers get the better of your company's network."

Additionally, Total Networks offers two-factor authentication services which can make phishing attacks less dangerous. With two-factor authentication, your team will need to enter in a secondary credential in addition to their username and password. These are often sent to a secondary device which prevents a hacker from accessing it. This secondary credential is often sent to a phone in a text message, but you can also rig it to send automated voice calls, and much more. Whatever you choose to do, these messages provide an extra hurdle for hackers, making it vastly more difficult to access your important data.

Don't let hackers get the better of your company's network. Give the real IT pros at Total Networks a call at (602)412-5025 to show cybercriminals you mean business.

Share this Article!
http://bit.ly/1H7qd27

It's Easy to Forget about Quality IT Service, and That's Okay

When it comes to service jobs, there are two kinds: Those where the work is highly visible, and those where work gets accomplished behind the scenes. Each service is valued and needed, yet, one may receive more attention and recognition than the other. Managed IT service falls under the latter category, and we're totally okay with that.

How do you know if we're doing our job correctly? If you don't physically see us at your office managing and maintaining your company's IT infrastructure, does that mean that we're not doing anything? Absolutely not. With Total Networks's managed IT service, we're monitoring your systems around the clock and constantly taking care of a variety of IT issues so that your systems run as smooth as can be. Due to the nature of this kind of preventative service, it's easy for you to forget about us, and that's kind of the point.

For those of us at Total Networks, it's not like we're antisocial or that we don't value the company of your business. Instead, it's our prerogative to stay behind the scenes. This approach keeps us out of your way while we do what it takes to get the job done. As odd as this sounds, when it comes to preventive IT care, lack of interaction with those we serve is how we gauge success.

"This approach keeps us out of your way while we do what it takes to get the job done."

This idea is communicated in a mantra that we've been going by for years, "Making Technology Work for You." The entire point of technology is that it's meant to enhance your goals and improve the efficiency of your business. If you have to spend time resolving technology issues, or even managing IT technicians that are on your premise, then that's time taken away from running your business, which negatively affects your bottom line.

When it comes to service jobs, there are two kinds: Those where the work is highly visible, and those where work gets accomplished behind the scenes. Each service is valued and needed, yet, one may receive more attention and recognition than the other. Managed IT service falls under the latter category, and we're totally okay with that.

How do you know if we're doing our job correctly? If you don't physically see us at your office managing and maintaining your company's IT infrastructure, does that mean that we're not doing anything? Absolutely not. With Total Networks's managed IT service, we're monitoring your systems around the clock and constantly taking care of a variety of IT issues so that your...

Read the rest Online!
http://bit.ly/1H7oWI9

Unfamiliar with BYOD? Here's Where to Begin

A trend that's taking the office by storm is BYOD, or Bring Your Own Device. These policies entail workers bringing their own devices to the office and using them for work-related purposes. While this opens up many avenues for enhanced productivity and efficiency, being too laissez faire with your BYOD policy could instigate some problems later on, primarily in the security field.

Why BYOD?

Before diving head-first into BYOD, you should take a moment to consider why you want a BYOD policy in the first place. If you're concerned about your team using their personal devices for work because you think they'll waste time playing games, perhaps a BYOD policy might not be the best solution for you and your business. If you're allowing your team to bring their devices to work, you need to be prepared to take certain steps to guarantee productivity and security. Additionally, the Internet of Things complicates the nature of BYOD. More devices are connected to the Internet than ever before. In light of these complications, you might feel that BYOD is a security discrepancy, at best.

However, contrary to some opinions out there, BYOD has incredible potential to be beneficial for your business's operations. With BYOD, your team can feel encouraged to work more hours, especially from the comfort of their own home. Additionally, some employees find themselves more productive using their own familiar devices rather than the foreign company-provided machines. Finally, being able to use their own devices can be a significant morale booster for your team, and you know what they say; when you feel good, you work even better.

Integrate Solid Guidelines

Integrating a BYOD policy into your business strategy is one that requires precision and careful thought. More often than not, it requires a dedicated project manager that knows their way around the industry. If this is your first foray into the unknown wilds of BYOD management, it'd be best to contact Total Networks and let our trusted technicians help you find your way forward.

As for a general pointer, one of the best things you can do is to set up specific guidelines that your team should abide by when using their devices for work. Without set-in-stone rules that can be applied company-wide, you risk the chance of someone being out of the loop, and therefore, not abiding by the rules you've put in place for your organization.

Mobile Device Management

It can be time-consuming and difficult to integrate your own BYOD policy, especially if you aren't sure how to approach doing so. A mobile device solution from Total Networks can make these difficult decisions for you. In order to maximize security, the mobile device management solution can perform these functions:

- **Limits network access to secured wireless devices.** With a BYOD policy, you'll have a lot of new devices attempting to access your network. It's important that only devices which have been approved have this access. Otherwise, you might be opening up your network to a whole new host of threats.
- **Whitelists and blacklists applications.** Certain applications request...

Read the Rest Online!
http://bit.ly/1H7rLcp

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

Bill Fox
VP, Customer Service

Total Networks

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

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

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