TECHMinutes

September 2017

Your Small Business Technology Information Source!

This Issue:

Labor Day 2017

In observance of Labor Day, our office will be closed on Monday, September 4, 2017.

We wish you and your families a safe and happy holiday.

Please be aware that emergency support will be available for our managed service clients.

A strong password is your first line of defense! Changing your password is more of a precautionary feature than actual security because, if someone has hacked you, they then have access to your data. Changing your password ends their access: thus by changing it regularly you limit the time attackers have to do damage. **Follow the link for a FREE poster of the above graphic!**

http://dti.io/underwear

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 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

(Continued on page 3)

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.

(Continued on page 2)

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 enterprise-level security solutions on the market into one convenient package especially made for small businesses. A UTM contains a firewall to keep dangerous traffic from entering (or leaving) your network, as well as an antivirus solution that can detect and eliminate threats that have made their way into your infrastructure.

Furthermore, preventative measures such as spam blocking and content filtering limit your organization's exposure to dangerous entities by blocking suspicious messages and inappropriate websites.

If your organization wants to take network security seriously, you need to understand that security shouldn't be reactive. Instead, you want to take proactive measures to prevent issues.

To learn more about what we can do for your business' network security, reach out to us at 607.433.2200.

Share this Article!
http://dti.io/looking

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

(Continued from page 1)

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 mindset leads to even more revenue spent on repairing systems due to one major factor: downtime. When an issue becomes a problem that keeps your employees from doing their jobs, it becomes quite costly.

Organizations that take advantage of break-fix technology maintenance are more likely to experience trouble in the long run compared to proactive managed services. By preventing issues from evolving into major problems, you are effectively saving money by keeping downtime to a minimum.

Directive specializes in preventative solutions designed to help your organization save time and improve IT maintenance. To learn more, reach out to us at 607.433.2200.

Share this Article!
http://dti.io/3trends

What Makes Managed IT the Best Option?

(Continued from page 1)

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 Directive a call at 607.433.2200.

Share this Article!
http://dti.io/option

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
- Communications (network and telecommunications)
- Data files and vital records
- Operations processing equipment
- Office equipment

General: These few items are very important to business continuity, but are frequently overlooked during the planning stages.

- Official Disaster Declaration
- Alternative Location
- Automated Systems Run Manually
- Maintenance of Plan
- Practiced Execution of Plan

For many small business owners, the realization that a lack-luster data backup solution does not constitute a...

Read the Rest Online!
http://dti.io/tipsbc

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...

Read the Rest Online!
http://dti.io/stats

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 ideal operational efficiency. The traditional way of acquiring these pieces of software can be holding your organization back, so we've come to you with a solution: Software as a Service (SaaS).

Normally, you would pay for a single software license. Doing so presents your company with a rather high up-front cost for the software, making the total cost quite considerable if you need a lot of licenses. While businesses can take advantage of certain perks, purchasing software per license isn't necessarily the best way to do it--not when you have other options available.

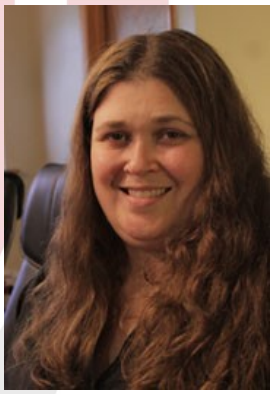
Another issue entirely is the fact that you have to continuously upgrade and purchase new software licenses for each of your business's workstations, particularly when your older solutions grow outdated and unsupported. This is yet another cost of implementing your business's mission-critical applications in the traditional fashion. While you might own your software license outright, it will only last for so long before it must be replaced.

Compared to traditional software purchasing, Software as a Service allows you to pay a flat monthly rate per user. The advantage of this is crucial for a small business that wants to get the most out of their investments. Rather than pay a large cost outright for your software licenses, you pay per user each month, which is a...

Read the Rest Online!
http://dti.io/saas

We partner with many types of businesses in the area, and strive to eliminate IT issues before they cause expensive downtime, so you can continue to drive your business forward. Our dedicated staff loves seeing our clients succeed. Your success is our success, and as you grow, we grow.

Chris Chase
Solutions Integrator



Charlotte Chase
Solutions Integrator

Directive

330 Pony Farm Road
Suite #3
Oneonta, NY 13820
Toll-Free 888-546-4384
Voice: 607-433-2200

Visit us **online** at:
newsletter.directive.com

newsletter@directive.com
facebook.directive.com
linkedin.directive.com
twitter.directive.com
blog.directive.com
instagram.directive.com