

This Issue:

Don't Forget to Renew Your Software Licenses

4 Old Internet Protocols Increasingly Vulnerable to Hacking Attacks

Windows Server 2003 End of Support Date is Fast Approaching

Introducing Cloud Computing to Your Business

The 3 Ways to Resolve a Technology Issue

Windows Server 2003 End of Support Date is Fast Approaching



Technology has come a long way since 2003. It seems like just

yesterday that Microsoft dropped support for Windows XP, and in just a few short months, they'll be dropping support for Windows Server 2003, as well. If your business is one of the many still utilizing this server operating system, you'll want to make sure that you upgrade away from it before July 14th, 2015.

(Continued on page 4)

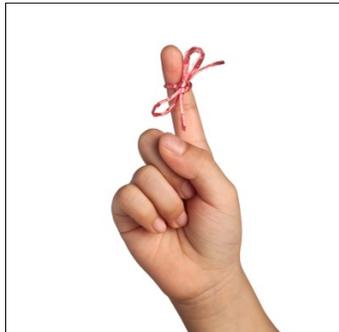
About Directive

We are a technology consulting firm specializing in technology implementation and management for businesses. We're known for providing big-business, Enterprise-Level IT services to small and medium-sized businesses.

Visit us **online** at:

newsletter.directive.com

Don't Forget to Renew Your Software Licenses



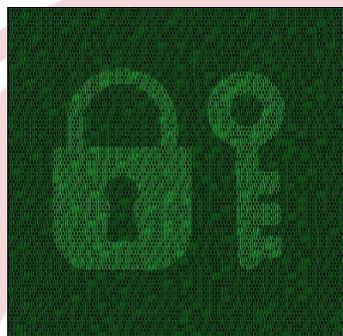
You have a system in place to remind yourself of when to pay your bills. Otherwise, bills would go unpaid, essential services would be cut off, and your credit rating would plunge. However, not everyone has a system in place to renew their software licenses, which could lead to consequences that are just as dire.

Many software users are dependent upon notifications from the software itself to remind them when it's time to renew. These notifications are sufficient for most users, but then there are the users that receive so many notifications from all over the place that they've grown numb to them. A user that clicked on "Don't show me this again," may miss out on crucial notifications about renewing their software, which could unintentionally lead to its expiration.

When a software license expires, it's likely to become unusable. This can be a major inconvenience if you're in the middle of a workday. One moment your staff is cranking out work using a mission-critical program, but the next moment, the software expires and everyone is locked out of their work. Granted, this isn't as severe of a downtime issue as a server going down; nevertheless, it's still a downtime issue that can cost your company money.

(Continued on page 3)

4 Old Internet Protocols Increasingly Vulnerable to Hacking Attacks



When the Internet was first established, malware and hacking were in their infancy, and not as much of an immediate problem as they are today. Thanks to this fact, the Internet wasn't really created with a certain security design in mind, and has instead adapted to shifts in its environment. Unfortunately, as hackers grow more powerful, several of these patchwork protocols are growing outdated.

While some of these protocols have been fixed routinely over the years, it's only growing more evident that these will require a more powerful fix sooner or later. According to InfoWorld, here are some of the more important protocols which are growing outdated with each passing year.

Border Gateway Protocol (BGP)

BGP is one of the more prominent protocols used in the modern technology world. Internet routers use this to exchange information over networks. Since it's been around since the beginning days of online computing, it's necessary to proper online function. However, it hasn't evolved to change with the times, and is vulnerable to being exploited for malicious activity. This type of attack happens when a hacker forces the device to route the network traffic elsewhere (for example, a malicious website). These types of attacks have happened in the past, and will continue to appear until a more effective protocol is found.

(Continued on page 2)

Introducing Cloud Computing to Your Business



You've probably heard about the cloud and how businesses are taking advantage of it, but due to the

way it's marketed and all the different tasks that it's capable of, there may be some confusion as to how it works and how exactly it can be a game-changer for your business.

At Directive we hope to clear this up a bit. The cloud takes some of your existing IT infrastructure and eliminates it from your office. Cloud computing comes in many different shapes and sizes based on your needs. For example, here's a quick overview of cloud computing's three most popular models.

- **Private Cloud Computing:** With the private cloud, a business will utilize

their own IT equipment to take advantage of the conveniences of cloud services. Companies that build and maintain a private cloud infrastructure have more control over their data. Businesses that store their data on a private cloud computing network is responsible for their own security and maintenance.

"...cloud solutions can handle your data storage, replace servers, and even dish out desktop environments so your employees can access their data from anywhere..."

- **Public Cloud Computing:** With the public cloud, businesses migrate their entire IT infrastructure over to a public cloud service. This form of

cloud computing is driven by lower costs and higher levels of convenience. Since public cloud services are a subscription service, there's a risk of being overcharged if entire private networks are migrated without adequately putting thought into which IT services may be best served if hosted in-house versus publicly over the cloud.

- **Hybrid Cloud Computing:** Then there's hybrid cloud computing, which combines aspects of both the public and private cloud. This hybrid cloud model allows for companies to store their sensitive data on a private cloud without risking their network exposure to the outside, while still making use of external resources to run applications that need this data. For many SMBs, a variation of this hybrid cloud computing model is the best option.

(Continued on page 4)

4 Old Internet Protocols Increasingly Vulnerable to Hacking Attacks

(Continued from page 1)

Simple Mail Transfer Protocol (SMTP)

The modern business also relies on email, which is reliant upon a protocol called SMTP. At the time the Internet was created, it was the easiest way to transfer mail via the web. As previously mentioned, SMTP was created before the Internet exploded with threats, so it's only natural that vulnerabilities to new and more dangerous hacks would arise. While various fixes are available, it's ultimately up to the network administrator to ensure that SMTP is as secure as it's supposed to be.

Domain Name System (DNS)

The same protocol that breathes life into your website is also fundamentally flawed, thanks to the efforts of hackers all over the world. DNS is what's responsible for taking your website's IP address and connecting it to your domain name. For example, by exploiting a vulnerability

in the way DNS functions, the Iranian Cyber Army managed to redirect Twitter's traffic to an entirely different domain hosting a defacement page. While multiple attempts to fix this issue with DNS have been made in the past, some can affect the performance of the DNS server itself; as such, a fix is still in the works.

Secure Sockets Layer (SSL)

You might recognize this one, especially if your site utilizes a security certificate. SSL was an encryption protocol designed to keep data transfer private both to and from the network. The problem here lies in the fact that SSL hasn't received an upgrade since 1996, and in light of the recent vulnerability found during the POODLE attacks last year, the world's most popular browsers (Google Chrome, Mozilla FireFox) are thinking of scrapping SSL altogether. Unlike these other protocols, SSL already has a replacement:

Transport Layer Security, or TLS. This means that SSL support is on its last leg, as it should be.

While the integrity of the Internet itself can seem questionable at times (especially considering the state of its protocol), your company's own security standards don't have to be. Directive offers managed IT services designed to prevent and protect your business from threats which might target your business's data infrastructure. Our Unified Threat Management solution (UTM) comes complete with a firewall, antivirus, spam-blocking, and web filtering solutions to keep dangerous entities away from your network. For more information about our UTM or other managed IT services, give us a call at 607.433.2200.



Share this Article!
<http://bit.ly/1FHn2PS>

Don't Forget to Renew Your Software Licenses

(Continued from page 1)

Consequently, if your accounting department isn't able to quickly renew the license for your expired software, then the time lost to being locked out of a needed program will make the downtime that much more expensive. A situation like this could have easily been prevented if the software license was renewed before its deadline.

If you're having trouble managing the renewal dates for all of your different software, then we've got a handy-dandy tip for you: Renew every program's li-

cence on the same day. Setting this up is as easy as contacting the software company and letting them know that you want to change your renewal date. You may have to pay a few extra months ahead in order to change this date, but given the fact that you're offering the software company money, they should be more than willing to accept your funds and change the renewal date to when you want it.

For the best way to make sure that all of your software licenses are renewed when they're supposed to be, you can

have Directive manage your software licenses for you. With our managed IT services, we keep track and manage all of your software licenses. This way, you won't suddenly get hit with an expired software and lose precious productivity.

To have one less IT maintenance issue to worry about, reach out to Directive at 607.433.2200.



Share this Article!
<http://bit.ly/1FHIW6x>

The 3 Ways to Resolve a Technology Issue



You know that one unlucky employee that seems to have the most problems with their computer? Perhaps they keep

getting an error that no one can replicate, or they need a little help setting up a Mail Merge? Due to most managers only knowing of two technical support options, business owners can get stuck in a tough spot with employees like this.

Option 1: Have Them Fix it Themselves

By letting an employee that's not skilled in PC repair sit at their desk and try to deal with the issue themselves, a lot of time will be wasted. Sure, they're bright and can likely figure out how to fix the problem by Googling the issue and watching how-to videos on YouTube, but that's not why you hired them. Plus, this DIY method will eat up a lot of company time.

You hired their bright mind to spend time and energy coming up with new and better ways to make your business money. Therefore, having an employee take time to learn about and fix a PC problem on their own will actually end up costing you double. It will cost your

organization for the time they spend resolving the issue, and the time they don't spend generating revenue for your company.

Option 2: Have Them Call Up Technical Support

The other option typically given to employees that are prone to breaking their technology is to have them call up the official technical support associated with the piece of broken tech. Granted, this is a much quicker way to fix a problem, but it's also a quick way to ring up huge technical support bills that just aren't in your budget.

"...they're designed to make money for themselves by charging a rather exorbitant fee to give their expert advice. Using these hotlines, businesses end up paying for an over-priced technical service..."

When it comes down to it, ordinary technical support services aren't designed with the intention of saving businesses money. Instead, they're designed

to make money for themselves by charging a rather exorbitant fee to give their expert advice. Using these hotlines, businesses end up paying for an over-priced technical service simply because they're unaware that there's a better way.

Directive's Third Option

We're here to pull you out of this lose-lose situation. We offer helpdesk support that allows you to encourage your staff to reach out to us if there's a technical problem keeping them from getting their job done. This means an employee isn't going to rack up a huge surprise bill and you'll be able to focus on growing your business, instead of prioritizing what gets fixed.

We couple this with our remote monitoring and maintenance IT service, which means all of your computers are already being taken care of. To prevent issues before they affect your bottom line, we encourage you to contact us today at 607.433.2200. Don't let a frustrating computer issue stop your staff from doing what you pay them to do!



Share this Article!
<http://bit.ly/1zS6GTM>

Introducing Cloud Computing to Your Business

(Continued from page 2)

As you can see, cloud computing isn't a one-size-fits-all solution, which is why many businesses have trouble implementing the cloud. A business that simply tells a cloud service provider, "We want the cloud," without first taking the time to learn about the different cloud computing models and cloud service options, may end up with a public cloud when a private cloud is a better fit, or a hybrid cloud when they really need a public cloud offering, or any

other cloud scenario that's just a wrong fit.

Directive can migrate your IT needs to the cloud, leaving IT maintenance and management responsibilities on us, while freeing up space, lowering utility bills, and greatly reducing the overhead of having to handle all your IT needs in house. Depending on your needs, cloud solutions can handle your data storage, replace servers, and even dish out desktop environments so your employees can access

their data and applications from anywhere and on any device.

If you're looking to save money, reduce your overhead, and free yourself so you can focus on your business, instead of your technology, contact Directive today at 607.433.2200 and ask us about our cloud solutions.



Share this Article!
<http://bit.ly/1721hyc>

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.

Windows Server 2003 End of Support Date is Fast Approaching

(Continued from page 1)

Otherwise, you'll be running without security patches or updates.

It should also be mentioned that Microsoft will offer custom support for those who can't make the upgrade in time, but it comes at a steep cost. Processor magazine estimates that it could potentially run businesses up to \$200,000 a year, making it an expensive alternative to simply upgrading to something more secure and reliable. Seeing how the last Service Pack it received was several years ago, and all

other support for the operating system has long since ended (it's currently on its last leg of extended support), upgrading now before it's too late is the optimal choice.

Whether or not you should upgrade isn't in question. You can't ignore security or compliance issues which arise from using an outdated operating system. Without the necessary security patches and updates, you're taking unnecessary risks which could potentially compromise your business. It's of the utmost importance that you keep your

infrastructure as secure as possible from outside threats, especially if you deal with sensitive information, like health records or confidential files.

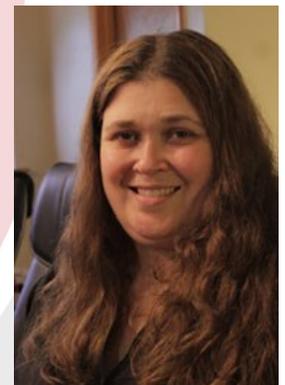
This begs the question, "How should I approach upgrading?" It depends on what kind of mission-critical applications your business is running. Some of your applications might have trouble migrating...



Read the Rest Online!
<http://bit.ly/1Em9ic2>



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



newsletter@directive.com



facebook.directive.com



linkedin.directive.com



twitter.directive.com



blog.directive.com

Visit us online at:

newsletter.directive.com

