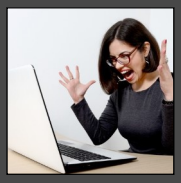
CELERANETWORKS
Making Technology Work For You

TECHMinutes
May 2016
Making Technology Work for You

This Issue:

3 IT Shortcomings That Drive Employees Crazy, and What You Can Do About Them



For small and medium-sized businesses, technology management can be a tricky situation. You want to ensure that your IT doesn't break your budget, but you also want to make using your technology as easy as possible...

Read the Rest Online!
http://bit.ly/1Nq9NWt

About Celera Networks

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.celeranetworks.com

How to Prevent the Crippling Effects of Downtime

Downtime is a critical problem with many businesses that have limited IT budgets. Organizations need to ensure that their bottom line is as high as possible, but if you're constantly plagued by persistent downtime, your business is losing money when it doesn't need to. We're here to inform you about downtime, and what it can cost your business if it's not addressed promptly.

Downtime, as reported by the Gartner IT Glossary, is "the total time a system is out of service." This could be the result of an unexpected hardware failure, a Distributed Denial of Service attack (DDoS), or even from the theft or destruction of critical data as a result of a virus or other threat. Regardless, any situation where your systems are left offline and inoperable for an extended period of time, could have devastating effects on your business.

To put it in simpler terms, **any time where your systems aren't running, is time that your team isn't working**. It's time where your servers aren't collecting data. It's time where your business isn't collecting new leads. Downtime is equivalent to lost profits and opportunities,

(Continued on page 3)

How Cloud Computing and Virtualization Can Free Up Your Business to Do More

The cloud is revolutionizing the way that businesses store and manage data, applications, and even abstracted hardware like servers and desktops. However, some businesses are still reluctant to adopt the cloud, despite its overwhelming advantages for small and medium-sized organizations. Therefore, we're taking it upon ourselves to "demystify" the cloud, so you can see just how great of an innovation it is.

What Is Cloud Computing?

Cloud computing is the act of storing information or data in an online environment. Basically, the cloud is a computer (or series of computers) managed and maintained by an external party, and your business receives its data and applications directly from it through the Internet. It's great for quickly and efficiently allowing your team to access specific information and programs that they need to get their job done properly. Examples of cloud computing services include data storage, application access, and even server hosting. Many businesses use it to store their productivity suite, like Google Apps or Microsoft Office 365, and to store data so that all of their employees have access.

How Virtualization Works

Virtualization is the act of taking multiple pieces of your network, like servers or desktops, and running them on a single piece of hardware. By doing so, you eliminate the physical costs of running and maintaining multiple, and often underutilized devices. **Your business can save considerable capital by investing in virtualization services designed to eliminate unnecessary physical clutter and overhead costs.**

(Continued on page 2)

Ransomware: A Look at Today's Worst Cyberthreat

There are many types of malware out there, but none that are quite as scary as ransomware. Imagine being struck by a threat that instantaneously locks down your files and keeps you from accessing them until you pay a certain amount of money. If your business is targeted by ransomware, would you be able to protect it from dragging your operations into a bitter pit of despair?

Ransomware is a malicious threat that has the potential to end your company's operations by eliminating access to critical files. It works by encrypting the files located on your PC, and the only way to get the decryption key is to pay the hackers who infected your computer. In 2015 alone, ransomware cost users over $325 million, which makes it an exceptionally lucrative venture for hackers. Ransomware generally worms its way into your PC through infected email attachments disguised as invoices or statements (i.e. phishing attacks), which means that inexperienced users might accidentally fall for the trick and unknowingly expose their PC to this threat.

Many types of ransomware will try to coerce money out of users through fear. For example, one variant of ransomware will pose as the Federal Bureau of Investigation, which might claim that the user illegally downloaded copyrighted material or is in possession of incriminating pornography. Others might claim to be from local law enforcement, demanding that a fine be paid in return your files. Some don't even bother trying to pose as other parties, and instead will simply make a demand that's quite difficult to resist: either you pay up, or your files are gone for good.

The most well-known type of ransomware these days is Cryptolocker, which locks down the files on a user's PC and demands a ransom. This ransom is usually to be paid in Bitcoin through the anonymous web browser, Tor, which makes it difficult, if not impossible, to trace the hackers' activity back to them. A more recent version of Cryptolocker, Cryptowall, is even more dangerous for businesses, as it allows infected PCs to spread the ransomware throughout the network they're connected to. This means that the all it takes is for one system to get infected for your entire network to be encrypted and held hostage by hackers. This isn't a situation you want to be in.

If your files are backed up somewhere, you should be able to eliminate the ransomware by restoring your backup. If your files aren't backed up, however, you might feel like there's no choice but to give in. The important thing to remember about ransomware is that you shouldn't pay the ransom under any circumstances. In the worst case scenario, you could pay the ransom and the encryption key might not work, putting you at a severe disadvantage. This would be no skin of the hacker's back, after all, they got your money. If you're ever infected by ransomware, it's important that you immediately disconnect your PC from the Internet and any network it's connected to, and to then contact trusted technology professionals. You do have options...

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

How Cloud Computing and Virtualization Can Free Up Your Business to Do More

(Continued from page 1)

A real world example of this is deploying a user's desktop from a centralized or hosted server, meaning you can broadcast it to any type of hardware, whether it's a laptop, thin client desktop, a home computer, or a tablet. It gives the user access to their files and applications regardless of the device they are using. In other words, you aren't bound to a specific computer or device.

How are Virtualization and Cloud Computing Related?

Like we mentioned earlier, a cloud is essentially just someone else's computer that you entrust your data and applications on. So the real question is how can this be more cost effective?

By taking advantage of high-end, expensive hardware and utilizing virtualization to get the most out of the hardware, a cloud provider can effectively provide computing resources for more users per capita. On top of that, the cloud infrastructure can be managed and monitored effectively by the provider's in-house team.

When it comes to the management and maintenance of your mission-critical systems, what would you rather have; your in-house team spending valuable time and revenue maintaining your in-house IT network, or an outsourced team of IT professionals who care for your technology just as carefully as they would their own? If your business wants to achieve its maximum potential, you need all hands on deck to implement and innovate with new initiatives. Our team of trusted professionals can give you the breathing room you need to ensure your IT goes smoothly.

Our professional IT technicians can help your business choose and implement the cloud solution that best fits the needs of your business. We can also assist your team with virtualization services needed to maximize your bottom line and limit unnecessary costs in your budget.

For more information about cloud computing and how we can help your business fully leverage its technology, give Celera Networks a call at (617) 375-9100.

Share this Article!
http://bit.ly/1Nq6VJl

How to Prevent the Crippling Effects of Downtime

(Continued from page 1)

both of which can hurt your business in the long run and hinder its growth. As reported by NetworkComputing, an estimated $700 billion is lost every year due to information and communications technology outages. Included in this number are lost employee productivity, lost revenue, and the cost of resolution.

There are several causes of downtime, but one of the worst is hardware failure or problems with your equipment. Many organizations still use the same technology they've been using for the past five, or even ten years, which can be a major detriment and an unnecessary risk. This is most often the case if a small or medium-sized business doesn't have the funds on-hand and readily available to regularly upgrade hardware and software solutions. If your business has a downtime problem, you should look into solutions that are capable of getting your systems back online as quickly as possible following a crippling disaster. One of the most critical components of doing so is a Backup and Disaster Recovery solution, otherwise known as a BDR device. BDR can protect your business's assets in the event of a catastrophic data loss or theft scenario. BDR takes multiple backups daily, allowing for minimal data loss. This data can then be deployed to your systems via the cloud, allowing for a swift recovery process that minimizes downtime. In fact, the BDR device can temporarily act as your server while you work toward getting a downed server back online, effectively eliminating the cost of expensive downtime.

In general, taking proactive measures to guarantee the minimum amount of downtime possible are encouraged, especially when it comes to the IT of small and medium-sized businesses. Monitoring your systems to ensure that no critical system failure is approaching is a good way to stay on top of your IT budget. Outsourcing this responsibility to a third party whose sole job it is to handle these issues is the ideal way to approach proactive IT maintenance.

Celera Networks can equip your business with both a Backup and Disaster Recovery solution, as well as remote monitoring and maintenance. We can spot the telltale signs of minor issues before they blossom into big, ugly problems that can cause expensive downtime. Trust us; your budget will appreciate it.

Share this Article!
http://bit.ly/263iVvU

The Future is Here: Domino's Now Has Pizza-Delivering Robots

Robotics are making leaps and bounds I n all sorts of different industries. Robots aid doctors with surgery, work in manufacturing plants, and perform countless other functions. Now, we can add "pizza delivery" to this list, thanks to a somewhat bizarre and extremely welcome innovation by the Domino's pizza chain.

Domino's has announced that it will soon be able to take advantage of a charming little pizza delivery robot that can autonomously deliver pizza directly to people's front doors. Dubbed the Domino Robotic Unit, or DRU, the robot will debut in Domino's Australian sector. It might seem like a hoax, but the DRU is indeed real. Fast food chains are known to try crazy marketing tactics once in a while, like KFC Canada's bluetooth printer bucket, so it's not that far of a stretch that Domino's would try something ambitious like this. The DRU has been tested in Queensland, Australia, and might only be the first step toward a future where the pizza-ordering process is improved.

"Domino's has announced that it will soon be able to take advantage of a charming little pizza delivery robot..."

Supposedly, Domino's claims that the DRU can perform the following tasks:

- Follow a map to a destination.
- Navigate sidewalks.
- Avoid obstacles.
- Keeps your pizza hot while it delivers it to the specified location.
- Keeps your drinks cold.

Domino's has been working with an Australian defense robotics firm called Marathon Robotics to fine-tune the DRU for successful delivery. Marathon Robotics tends to produce moving targets for law enforcement, state defense, and so on, for use during training exercises. Basically, the DRU could be assaulted by criminals and take a beating, while keeping your pizza safe from hungry street hooligans.

Robotic deliveries and autonomous vehicles, while uncommon, aren't unheard of. For a while, Amazon wanted to take advantage of drone delivery services, but hasn't quite gotten their service "off the ground," so to speak. Still, the Domino's pizza delivery robot is the first of its kind, and will likely continue to push innovation forward for new and exciting pizza delivery tactics. t just shows that businesses will go to great lengths to use modern technology to their advantage.

Would you trust a robot to deliver a pizza to your front door? Let us know in the comments, and be sure to subscribe to our blog for the latest tech tips, news, and tricks.

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

Know When Your Windows OS Expires and Why it Matters

By design, Microsoft's operating systems aren't built to last forever. Due to the fact that technology is always changing, new operating systems with better security and improved capabilities are routinely needed. Microsoft gets users to transition from an older OS to a newer one by ending support for the older one. This begs the question, how long until Microsoft pulls the plug on your OS?

Before we provide you with a list of expiration dates, we first must clarify the difference between Microsoft ending mainstream support of an OS vs. ending its extended support. Think of it like this, instead of Microsoft abruptly pulling the plug on a widely used OS, they will instead phase it out with two end-of-support dates which are generally five years apart. Here's the difference between the two dates:

- **Mainstream support**: When mainstream support ends, Microsoft stops issuing non-security related fixes unless you have a previously-established extended support agreement. Warranty claims also end, and Microsoft stops accepting requests for new features or design alterations.
- **Extended support**: When extended support ends, Microsoft will no longer issue critical patches and security updates. When this happens, your systems will be exposed to vulnerabilities that won't be fixed. The only solution is upgrading to a more recent OS, or biting the bullet and purchasing exorbitantly expensive custom support from Microsoft.

Now that you have a grasp on the different kinds of support provided and taken away by Microsoft, here's the list of end-of-support dates that you came here for:

End of Support for Windows Operating Systems

- **Windows 10**: Mainstream support ends October 13, 2020, while extended support ends October 14, 2025.
- **Windows 8.1**: Windows 8.1's mainstream support ends January 9, 2018, and its extended support ends January 10, 2023.
- **Windows 8**: Windows 8 is no longer supported by Microsoft. To continue receiving patches and security updates, upgrade to Windows 8.1 or Windows 10.
- **Windows 7**: Windows 7's mainstream support ended on January 13, 2015, and its extended support ends on January 14, 2020.
- **Windows Vista**: Windows Vista's mainstream support ended on April 10, 2012, and extended support ends on April 11, 2017.

Now, just because you're running an OS that's currently supported by Microsoft, doesn't mean that your system is up to snuff. Microsoft only sends you the Windows updates and security patches; it's up to you to apply them. If you don't, then you're leaving your system vulnerable.

It's easy enough to apply Windows updates for your home PC, but it's another thing entirely to apply Windows updates across all of your company's workstations and server units, and verify that they've been applied....

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

We partner with businesses in many different vertical markets throughout the New England area. The Celera team is focused on customer service and we strive to eliminate IT issues before they cause expensive downtime.

Our goal is for our clients to continue to focus on what's most important - their business.

Our dedicated staff is known for going the extra mile and doing what it takes for our clients to be successful with their technology investments.

Your firm's success is our success.

Tech Fun Fact

About 1.8 billion people connect to the Internet, only 450 million of them speak English.

Celera Networks

11 Elkins Street
Suite 330
Boston, Massachusetts 02127
Voice: (617) 375-9100

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

facebook.celeranetworks.com
linkedin.celeranetworks.com
twitter.celeranetworks.com
blog.celeranetworks.com
newsletter@celeranetworks.com