This Issue:

5 Best Practices for Traveling With Technology

Do you find yourself traveling for your business? Be it for a conference, a series of meetings that require your attendance, or some other reason, you may very likely need to spend some time on the road; time that could be spent on tasks your business needs to function. Despite the lack of a traditional workspace, this time spent...

Read the Rest Online!
http://bit.ly/2cg6VWf

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

Why You Should Be Skeptical of USB Devices

USB technology is widely-used and you'd be hard-pressed to find an organization that doesn't utilize USB devices in some way, shape, or form. However, these devices often harbor unexpected threats that could put the security of your entire infrastructure in jeopardy. All it takes is one infected device to compromise your network. Do you know where your USB devices have been?

Since USBs are prized for their portability, they can be used for a myriad of purposes. USB flash drives or hard disk drives can be used to transport files, both compactly or in bulk. Many keyboards and computer mouses operate with USB technology these days. That's not even mentioning the plethora of USB dongles that are used to connect other devices to your computer.

Now, imagine this scenario. An employee finds a USB drive on the ground and, curious to find out what's on it, plugs it into their company-issued workstation. They might do this to make sure that good technology isn't just left lying around, or maybe their curiosity just got the best of them. Either way, the files on the device could contain executable malware that can threaten your business. In many cases, the user might not even be aware that malware has been installed on the computer, and it can spread viruses, or install Trojans

Is IT Innovation Driving, or Hindering, Your Business's Growth?

Technology can be a constant pain point for businesses of all kinds. Due to the ever-evolving nature of technology solutions, it's tempting to cave in and purchase the latest and greatest innovations in the industry. Yet, does your business have the time to do so, let alone the budget? Progress can be stymied by a lack of funds and personnel, but it doesn't have to be.
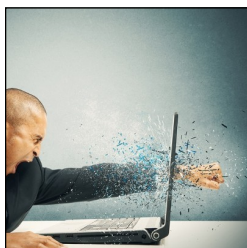
More often than not, businesses are stuck in two situations. Depending on the state of your IT environment, you either have plenty of time to implement new and innovative solutions, or you have, quite literally, no time to even consider new technology. Both situations come with side-effects that could negatively affect your organization's operations. For example, you might have time to implement new technology, but are you ignoring the day-to-day maintenance of your internal systems?

The latter can also be a major problem. If you're spending all of your time responding to emergencies, when can you implement new technologies that can potentially improve the functionality of your business? When you can't even handle the solutions you already have, what's the point in implementing new technologies? Unless you can find a way to strike a balance between the two, any efforts will be both fruitless and wasteful.

"Ransomware is more about manipulating vulnerabilities in human psychology than the adversary's technological sophistication" - James Scott

Page 2

How Much Money Does Your Business Waste on Slow Computers?

Have you ever been forced to use a slow computer out of necessity? This is a practice that tries more than just your patience; it can also put a drain on productivity, and in turn, your business's profits. Therefore, we'd like to ask you a very important question: can your business really afford to deal with technology that isn't performing as intended?

Oxford Economics and Nimble Storage suggest that the most productivity is lost due to what they call the App-Data Gap, which is defined as "the delay that occurs when someone interacts with a business application and the application's response time." Basically, it's just a fancy term for explaining how long it takes applications to load. The two companies asked 3,000 users around the world how slow computers affected their workflow, and the results shouldn't be surprising.

When asked if their technology held them back from achieving the maximum amount of work possible, a stunning two-thirds claimed that they were using sub-par technology that failed to let them unlock their true potential. The result was particularly high for the United States, at 76 percent.

Also of note is that respondents claim that they lose, on average, 48 minutes every day from working with slow technology. That's about 10 percent of the average workday, and it can lead to significant losses in the long run. ITProPortal estimates that United States companies lose out on $7.5 billion annually due to lost worker productivity from slow technology. However, unlike having employees that simply waste time out of habit, providing them working technology is something that you have control over.

We'd like to make an educated guess about why so many companies endure slow computers. Perhaps it's because they are small businesses that either can't afford the comprehensive support and maintenance their systems need, or their internal IT department doesn't have the time to perform maintenance when it's needed. In situations like these, outsourcing is often the best way to go, but how can you know for sure what tech support to go with?

Celera Networks understands what it means to be using slow or underperforming technology solutions. You're not just keeping your employees from getting work done; you're limiting their potential, frustrating them, and making it harder for them to make your business money. Plus, slow computers could also be a sign of other issues that may not be immediately noticeable.

Some online threats can eat up your computing resources and make operations drag, while other issues could be the result of an imminent hardware failure. It's up to you to respond to these issues and ensure that your technology gets the attention it needs.

If your in-house team simply doesn't have the time or expertise required to perform maintenance on your technology, we have technicians standing by to help your team resolve technology problems and optimize your organization's operations.

Share this Article!
http://bit.ly/2cg7tLs

Is IT Innovation Driving, or Hindering, Your Business's Growth?

One of the best ways that your business can innovate without sacrificing functionality is by taking advantage of outsourced IT solutions from Celera Networks. Whether you're in desperate need of a new workstation or server, or need to implement a solution on a large scale, like cloud computing or virtualization, our trusted technicians can help.

If your team can't keep up with maintenance, we can take over this responsibility while they innovate and create new solutions for your organization.

Better yet, you can rest assured knowing that you're getting top-of-the-line technology assistance for your organization's systems. More often than not, businesses have to cut corners in order to make ends meet with their technology maintenance, which could include allowing end-users to service their own workstations. This is a hazardous practice, as having inexperienced users performing in-depth maintenance could be both time-consuming and risky.

You can save time and money by allowing an outsourced team of technology professionals to work with your critical systems. Not only will you see a return on your investment in the form of better-functioning technology, but you'll also be able to rest easy, knowing that your systems are being maintained by qualified professionals who want to see you succeed.

If your business would rather implement its own solutions, that's fine too. We can sit on the sidelines and handle maintenance for you so that you don't fall behind. Regardless of what the internal status of your IT is, we are sure to have a service that's a perfect fit for your business.

Share this Article!
http://bit.ly/2cg7kbb

Why You Should Be Skeptical of USB Devices

(Continued from page 1)
that allow for remote access at a later date.

In fact, there's been a recent report from May 2016 of a $10 USB device that's capable of logging keystrokes on wireless Microsoft keyboards and transmitting the signals over a wireless frequency. Whitehat hacker Samy Kamkar built it out of a USB phone charger, which is so commonplace these days that nobody would think twice about seeing it plugged into the wall of your office. The threat of these types of devices is so significant that the FBI saw fit to issue a statement warning professionals of their dangers. While no attacks have been found in the wild, it's still best to

take the warning to heart and apply it to your own cyber security practices.

The root of the problem--the theft of data before it reaches its destination-- extends well beyond Microsoft wireless keyboards, too. Any wireless device that sends signals that aren't encrypted could potentially be intercepted by hackers using similar techniques. This method can be used to harvest data that could lead to the theft of personally identifiable information, login credentials, or financial credentials. It's not unlike a hacker intercepting data over an unsecured wireless Internet connection.

Is your business prepared to handle these outside-the-box threats? All it

takes is one mistake to expose your company's data to those who would do it harm. In instances like this, you should make a policy that any and all devices your employees want to use should first go through your organization's security protocol. This will help ensure that the devices are not threats to your critical infrastructure. Emphasize that your organization should only be using encrypted data storage devices whenever possible, and you can't go wrong.

For more information about how to keep your business safe, contact us at (617) 375-9100.

Share this Article!
http://bit.ly/2cg8za8

When IT Implementation Goes Wrong, Focus on End-Users First
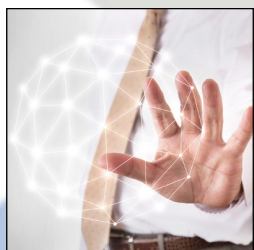
Often times, people can get distracted by flashy new features, and with technology, this happens more than anywhere else. Since IT grows at such an abnormally fast rate, end-users can be left in the dust if you're not intentionally trying to keep them in the loop. In fact, it's highly recommended that you implement IT solutions for your business that are not just effective, but also user-friendly.

The reasoning for this is simple: your end-users are the ones who will be using the technology. Therefore, you need to consider how they will react to new solutions, and whether or not it will be something that they can understand how to use. The first step toward improving the way that your IT infrastructure functions is by implementing solutions that are user-friendly first, and great technology second.

In fact, when organizations implement new solutions to increase productivity,

what they see is often the opposite. InfoWorld claims that this is due to two reasons: 1) Lack of training, and 2) A reluctance to change habits or behaviors. If your business implements new solutions, like an updated office suite or a brand new operating system, it will have little effect on your productivity if your team doesn't know how to properly use it. In fact, they may just resist the change altogether.

More often than not, your end-users will only care about one thing: functionality. They don't care how technically sound a solution might be, so long as it's simple to use on their end. Therefore, if you hope to get the most out of your new IT solution, you need to ensure that your team is both educated on the benefits, as well as competent in its usage. This can help to cut down on resistance to the project, as well as make it easier to hit the ground running once the implementation has finished.

InfoWorld states: "You might stagger the rollouts so the disruption is spread out. Rolling out a series of smaller changes takes more time, but it also lets users get more comfortable with the changes,

reducing the disruption to their work. It might even let some users get deep into new capabilities and share their excitement with colleagues, who won't be so overwhelmed with changes that they can't focus on the benefits."

The idea is to make your new IT solution not just a successful deployment for your IT department, but also for your users. This is what defines a successful solution deployment. After all, your end-users are the ones who will be using it, so if they get very little out of the solution, then why bother spending the time and resources implementing it?

If your organization is having difficulty implementing new IT, or training its team on how best to use your new technology, we can help. We want your business to succeed, and by helping you master your new technology solutions, we succeed ourselves.

To learn more, give us a call at (617) 375-9100.

Share this Article!
http://bit.ly/2cg8VO1

Cortana Gets a Little Too Clingy After Latest Update
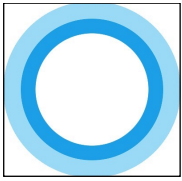
The idea of speaking to your device and having it perform tasks is hardly a new one. Siri and Google Now have long dominated this industry. Microsoft released Cortana in an attempt to enter the voice assistant race, but with Windows 10's anniversary update, more harm than good could come from using Cortana.

Since the release of Windows 10 last year, users have been quite vocal about Windows 10's innate settings. Some have argued that Windows 10 shares too much data and that Microsoft should address the problem. While this may (or may not) have been true, depending on who you ask, it doesn't change the fact that Microsoft's intentions were to provide a functional and user-friendly virtual assistant.

The main problem with Cortana is that you can't turn it off. The Windows 10 anniversary update, called Windows 10 SP1, disables this function. This is problematic, especially for businesses that require high-security measures.

If you can't turn off Cortana, she could be lurking in the background, watching your every move to target your device with ads tailored to your specific search history and activity. To make matters worse, the only easy way to prevent Cortana from collecting your device's data is to set it to avoid doing so when you install Windows 10.

If you're installing Windows 10 for the first time, we highly recommend against using the "Express Settings." If you use these settings, you might find that your user experience is more functional but overall less secure. The reason for this is simple; you can customize your settings and limit Cortana's access to information that could be sensitive, like your contacts, location, calendar data, email, and more. This resolution can also become another problem, though, in the form of Cortana losing out on almost all of its functionality. Can't Microsoft just give us a simple on/off switch?

Another issue that many organizations have with Cortana is its new feature that allows for the voice assistant to perform basic search functionality without the user logging into the device.

Think about it; any feature that allows any functionality whatsoever without the user being logged into the device can be considered a security risk. We think it's only a matter of time before this "feature" is exploited for gain by hackers and other malicious entities. In the meantime, you can turn this feature off by going through Cortana's settings and turning off the "Use Cortana even when my device is locked" feature.

Of course, there are plenty of security benefits to keeping Windows 10 updated, so completely ignoring the update isn't advisable either.

There are ways that you can turn off Cortana, but we don't recommend them to anyone who's not well-versed with the innards of the Windows operating system. If you have no clue what the registry does or looks like, chances are you should leave this to the professionals at Celera Networks. We want your organization to use the latest and greatest technology solutions, but we also want to help you stay safe and secure at all times when online.

To learn more about how to keep Windows 10 secure, reach out to us at (617) 375-9100.

Share this Article!
http://bit.ly/2cg7zCW

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