

This Issue:

Seasons Greetings!

3 Vendor Scenarios You Can Do Without

How Does the Cloud Affect Your Networking Strategy?

2 Important Networking Trends You Must Consider

5 Tips to Consider for Your IT Budget

The Most Dangerous Threats to Your Business Could Be Internal

1 Million Websites Not Using the Latest Security Protocol Soon to Be at Risk

How Does the Cloud Affect Your Networking Strategy?



Technology changes constantly, and as such it can be difficult to change and

adapt to new trends in the industry. Cloud services are making the implementation of scalable solutions somewhat easier, but often times...



Read the Rest Online!
<http://bit.ly/1Qp7A24>

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



On behalf of everyone at Celera Networks, we'd like to thank you for making this such a wonderful year, and we look forward to many more opportunities in the years to come. We truly appreciate you and your business. Sending the warmest of holiday wishes from our family to yours.

3 Vendor Scenarios You Can Do Without



Vendors can be a hassle. You need their product or service to keep the gears of business turning, but sometimes, having to deal with vendors can be way too time-consuming. This is where our vendor management service comes in.

With Celera Networks on your side, we can handle all technology vendors for you so that you don't have to. This is what it looks like to have a "single point of contact" for any and all of your technology-related needs. Image not having to deal with these three common technology vendor annoyances.

Vendor Acquisitions

The speed of business moves rapidly. Sometimes a vendor will go completely out of business, requiring you to find a new supplier. Other times, a vendor might get acquired by another company and your account will get mishandled in the transition. At the end of the day, you don't much care who bought out who and which company folded up; all you care about is keeping your business supplied with working hardware and supported software.

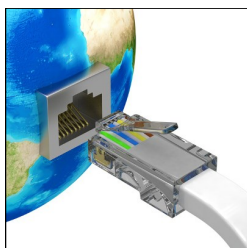
Instead of having to be bothered by business moves that are outside of your control, **let us coordinate your accounts to find you new, trustworthy vendors that best suit your needs.**

Drama with Your Vendor Account Manager

Have you ever dealt with a vendor point of contact that just happens to rub you the wrong way? Maybe they have a poor attitude, or maybe you've had a major disagreement with them in the past over-billing. Then there are some companies which seem to have a revolving door when it comes to their point of contact, which means that you've got to explain the particulars of your business to a new account manager way too often than you should have to.

(Continued on page 3)

2 Important Networking Trends You Must Consider



One sometimes-frustrating aspect about computer networking comes from the always-changing nature of technology. For example, let's say that you have your network perfectly set up with everything running smoothly, then comes along some new-fangled IT trend or mission-critical technology workflow that requires you to change everything. You can't prevent this from happening, but you can stay on top of the latest IT trends so that you're not caught off guard.

To that end, here are two IT trends that will cause you to make some major changes to your company's network.

Mobility (BYOD)

Business today is going mobile as workers utilize their personal devices for work purposes. Many companies are adapting to this trend and providing

their staff with mobile devices so they can get work done more efficiently. Providing devices for your staff takes away the worry that's inherent from the security risks of BYOD (bring your own device). In fact, in a recent IT survey by Forrester Research, "65 percent of respondents said they plan to expand their enterprise mobility services to meet their business priorities."

What this means for your business is that you're going to have to accommodate this trend, or else have your network be overwhelmed by mobile devices. One of the challenges of BYOD is that it opens the door to twice as many access points that all need to be managed and secured. Plus, you're going to need to increase your network's bandwidth, or else experience some major lag issues when the number of mobile devices accessing company files inevitably doubles.

Unified Communication and Collaboration

What you're sure to run into as you continue to do business in the modern age is

more companies and clients requesting meetings via video conferencing and other digital collaboration tools. NetworkComputing explains:

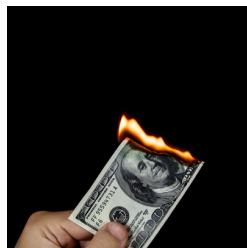
Communications and collaboration solutions now allow businesses to assemble the best people to do a job, regardless of their location. Information sharing between companies – in organizational settings; between suppliers, vendors and clients; or for special projects – has also become the norm.

If your business isn't equipped with these tools, then you're going to miss out on potential sales and networking opportunities, as well as a powerful way to streamline internal communications with your team. Equipping your network with a solution like Voice over Internet Protocol will give you the modern communication capabilities that you need, without crippling your current...



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

5 Tips to Consider for Your IT Budget



Think in the Long Term

When planning out your IT budget, it's important to consider both short-term and

long-term investments that you'll be making for the sake of your business. The fact that so many services, like cloud computing, are being turned into operational expenses, is placing an emphasis on a model based around affordable payments rather than heavy up-front costs. It's important to consider how these costs will affect your budget, especially over the long-term.

Invest in Training Your Staff

There's far too little investment in ensuring that employees understand the ben-

efits of the latest technology solutions. What good are the latest IT solutions if your staff has no clue how to use them? By properly training your team on how to take advantage of this technology, you're essentially providing them with skills necessary to make their workflow easier and more convenient. This helps them get the most out of their technology and maximize the amount of work they're able to perform.

Carefully Consider Storage Options

Your organization shouldn't just be taking advantage of one centralized storage system for its data. Instead, you want to have multiple avenues where your data can be stored. One of the primary reasons for this is because you need to make sure that your data won't be wiped out in one fell swoop (redundancy is crucial). Another reason for this is to

optimize your organization's access to its critical data. For this purpose, cloud computing can be exceptionally helpful, for both data storage and data backup solutions.

Account for Anticipated Software/ Hardware Upgrades

Unexpected hardware failure can be a pain to deal with, especially if your budget hasn't taken these issues into account. Not only are hardware failure and software issues hard to predict, but they're also expensive to replace. Your budget should always have assets allocated toward mitigating and replacing technology that's critical to the success of your business.



Read the Rest Online!
<http://bit.ly/1MGsvD6>

3 Vendor Scenarios You Can Do Without

(Continued from page 1)

Celera Networks can relieve this vendor drama by working with technology vendors on your behalf. One way that we do this is by taking the time to learn the intricacies of your business and what your needs are, which effectively makes us a liaison for your company's technology needs.

When You Experience Problems with Mission-Critical Technology Services

When you experience a problem with a mission-critical technology service like your Internet connection or cloud hosting service, it's on you to drop eve-

rything and call the vendor to get the situation resolved. TechRepublic offers this scenario which you may have experienced:

You consign a major system to a cloud-based vendor because the vendor has a reputation for being reliable and best in class—then the vendor has a failure that puts all your users offline and has a dire impact on [your] company's business.

When dealing with nightmare scenarios such as this, you're going to want a professional on the phone representing you. You need someone in your corner that's

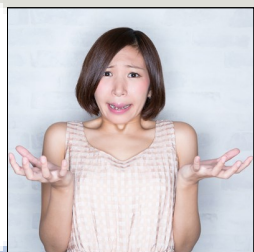
knowledgeable enough about technology to resolve the issue as quickly as possible. At Celera Networks, we deal with technology service vendors all the time and we know what it takes to get your company back online.

Alternatively, you could handle of these frustrating vendor issues on your own, but why would you if you don't have to? Call us today at (617) 375-9100 to have us be your single point of contact for all of your company's technology needs.



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

The Most Dangerous Threats to Your Business Could Be Internal



Most of the time, when it comes to cybersecurity, businesses tend to focus primarily on external

threats rather than those that might be lurking in the shadows of their internal operations. Believe it or not, the most dangerous entities out there could very well be working for you, right under your nose.

What Constitutes an Inside Threat?

While there are a number of entities that can threaten your business, many of them come from within. Included are previous workers who might not have left on the best terms, current employees who could be engaging in corporate espionage, or even unknowing end-users who might have allowed external hackers to compromise your network infrastructure.

- **Irate former employees:** Some employees will quietly pack their things and be on their way without saying a word. Others will make a big fuss and leave in a flurry of rage. It's the latter that you have to worry about, simply because they could lose their head and leak any information, like

passwords and whatnot, to the web. Or, if they're feeling particularly sneaky, they might attempt sabotage themselves.

- **Suspicious co-workers:** If there's some behind-the-scenes action going on in your business, you might suspect that someone internally is behind it. Issues like stealing equipment, devices, or even data, can arise for a variety of reasons. However, it's most likely for personal gain, like monetary compensation or to assist themselves with other endeavors outside of your business.
- **End-user error:** Unlike the previous two examples, workers who have made mistakes and cost the company its data security or worse don't necessarily do so on purpose. This can often be seen by the spear phishing hacker, who will target unsuspecting employees and coerce information out of them with phishing scams.

How You Can Protect Your Business

In order to ensure that your business follows a policy that mitigates insider threats, be sure to follow this action plan:

- **Integrate an office security system:** While this might seem like a far-fetched idea, it's a very common

occurrence in the small business environment. Organizations just like yours take advantage of security systems to ensure that nobody is breaking into the building, trespassing where they aren't supposed to, or taking part in any sketchy activity.

- **Monitor and maintain your access logs:** If you're concerned that there might be some suspicious activity on your network, you should integrate a comprehensive monitoring solution, complete with access logs that can tell you who accessed the network, from where, and when. This helps to keep only approved users from accessing the network.
- **Perform exit interviews:** When someone leaves your business, you should implement a thorough process to distinguish whether they own company devices or data, and respond to any concerns you or they might have about their departure. It also gives you a chance to address problems before they become serious issues later on. If someone is fired for seemingly no reason, they will grow bitter, and if they have sensitive information, it's perfectly reasonable to assume that they...



Read the Rest Online!
<http://bit.ly/1MGU9o8>

1 Million Websites Not Using the Latest Security Protocol Soon to Be at Risk



It's natural to replace older technologies with better, more recent

models. However, the future isn't looking too bright for the world's most common website encryption method, SHA1, which will soon be replaced by a more secure protocol. Pretty soon, browsers and devices may have some difficulty reading the latest security certificates, which could cause quite a problem if it's not remedied.

We're all familiar with the web encryption used by many sites out there: Google, Gmail, Facebook, Twitter, Microsoft, and so many more, all take advantage of HTTPS in order to provide a more secure web browsing experience. HTTPS is a signifier that the websites are using SHA1, which ZDNet describes as "the cryptographic hashing algorithm that's been at the heart of the web's security for a decade." In other words, it's thanks to this technology that the everyday user can safely use services with certainty that the web page hasn't been tampered with by hackers, who might be trying to skim websites for sensitive data.

Ordinarily, moving to a more powerful security algorithm wouldn't be a big deal. However, the issue at hand comes from users who don't have technology that's capable of reading these new security certificates. Though the number of those affected is relatively small compared to the total number of technology users, there are plenty of people out there who will be put at risk because they can't process the new SHA2 security protocol certificates. Thankfully, however, most websites that utilize security certificates are already taking advantage of the SHA2 encryption. As reported by ZDNet, "about 24 percent of SSL-encrypted websites still use SHA1 -- or, about 1 million websites."

This is a great step in the right direction, and the situation is improving every day. By the end of the year, it could reach as low as 10 percent, meaning that the likelihood that users will encounter a SHA1 site is extraordinarily low. Similarly, according to ZDNet, most users are using the most recent versions of their browsers and OS software anyway:

"For most people, there's nothing to worry about. The

majority are already using the latest Chrome or Firefox browser, the latest operating system, or the newest smartphone with the latest software, which are compatible with the old SHA1-hashed websites and the newer SHA2-hashed websites. But many, particularly those in developing nations, who are running older software, devices, and even "dumbphones," the candy-bar cellphones that have basic mobile internet, will face a brick wall, because their devices aren't up-to-date enough to even know what SHA2 is."

Basically, what it comes down to is ensuring that your business's devices are always up to date with the latest patches and security updates. If your operating systems and all of your software are using the latest version, the chances that you'll run into one of these issues is exceptionally low. The easiest way to make sure that all of your technology is up-to-date is by taking advantage of Celera Networks' remote monitoring and maintenance solution, which can make this daunting task much more manageable by handling...



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

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

Mosaic was the first popular web browser, which was released in 1993.

Celera Networks

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



facebook.celeranetworks.com



linkedin.celeranetworks.com



twitter.celeranetworks.com



blog.celeranetworks.com



newsletter@celeranetworks.com

Visit us **online** at:

newsletter.celeranetworks.com

