



**This Issue:**

Total Networks' Senior Engineer David Rice Earns Security+ Certification

Security Problems That Shape the Way Businesses View Cybersecurity in 2015

Windows 10 Is Just Around the Corner, But What's the Demand?

How Fast Can Your Business Recover from a Data Breach?

If Only Managed IT Service Extended to Your Car

3 Ways Your Business Can Benefit from a Private Cloud Solution

How to Properly Store a Hard Drive

**Windows 10 Is Just Around the Corner, But What's the Demand?**



Just because something is brand new doesn't mean that there's a market for it.

Just look at Windows 8 to see what we're talking about. It might have been a brand new operating system when it first came out, but it didn't really take to users, who



Read the Rest Online!  
<http://bit.ly/1M6icld>

**About Total Networks**

Building on the tradition of providing industry best solutions, the Kinseys continue to invest in tools, training, recruiting, and procedures, continuing to extend our reputation as the premier IT service provider in Arizona.

Visit us **online** at:  
[totalnetworks.com](http://totalnetworks.com)

**Total Networks' Senior Engineer David Rice Earns Security+ Certification**



David Rice continues to add to the stack of training certifications for Total Networks' resume. Not only has he achieved three Microsoft Certified Professional certifications in the last year (Windows Server 2012, Server 2012 R2 MCSA, and Microsoft Exchange Server 2013), David has recently achieved the CompTIA Security+ Certification.

The CompTIA Security+ certification designates knowledgeable professionals in the field of security, one of the fastest growing fields in IT. The CompTIA Security+ accomplishment demonstrates David's

knowledge of the most important principals for securing a network and managing risk. The certification is approved by the U.S. Department of Defense to meet IA technical and management certification requirements.

Security and other IT certifications are important to Total Networks. "It's critical that we stay up to date on the latest technology, I am proud to have a strong team that is committed to ongoing education", notes Total Networks President Dave Kinsey.

Recently Total Networks received the CompTIA Security Trustmark™, a respected industry credential that signifies its adherence to best practices for information security.

"Earning the Security Trustmark is validation of our efforts to implement security practices to protect our clients' critical asset—their data," said Dave Kinsey, owner of Total Networks. "In today's world of hacking and data breaches, we have developed a Culture of Security at Total Networks that will pay off for our clients every day."

The CompTIA Security Trustmark was developed with the support of technology companies at the forefront of the IT security industry.

To earn the Trustmark Total Networks successfully passed an independent assessment of their security policies, capabilities, practices, and processes against industry best practices in areas such as security technologies; vulnerability assessment detection; data encryption; technical employee knowledge/expertise; security clearances and background checks; physical and hardware security; and permissions, passwords and other security requirements.

**Security Problems That Shape the Way Businesses View Cybersecurity in 2015**



So far, 2015 has been relatively calm compared to the hack-fest that was 2014. However, we're only halfway through the year, and there's still plenty of time for hackers to make short work of networks. Remember, all it takes is a single mistake to expose your business's network to a host of different threats. Understanding what these threats are and how to handle them is of the utmost importance.

Calyptix Security explains in-depth how some of these threats will react to the measures taken by even the most cautious businesses.

**Phishing Emails Often Pose as Your IT Department**

Hackers are thinking logically when it comes to phishing scams, and who better to impersonate

*(Continued on page 3)*

## How Fast Can Your Business Recover from a Data Breach?



How much thought have you honestly put into your business's data recovery procedure? It's likely that

you, like many other businesses out there, are taking a minimalist approach with both your data backup and disaster recovery. It's not that you aren't aware that they're a good thing; you might just feel that you don't need it because you feel hackers have no reason to compromise your data. Unfortunately, that's what hackers are counting on: complacency.

One of the many reasons your business needs a data recovery solution in place is data theft from hackers. If this occurs, you won't be able to access mission-critical information that's necessary for operations. That's not mentioning the compliance problems you'll find yourself in shortly following the breach, especially if sensitive customer information was stolen.

Naturally, the first thing you want to do in the event of a data theft is consult your current backup and recovery solution. However, you might be distraught if the recovery process is long, and you might run into complications if your data backups are out-of-date. While this is vastly superior to losing all of your data permanently, you want to recover as much data as possible in order to minimize your overall losses.

Furthermore, if your business has no discernible data backup and disaster recovery plan in place, you stand to lose everything in an instant. You should never underestimate the value of your business's data. A company normally holds onto financial information of clients, Social Security numbers of employees, and other sensitive information which can be very lucrative to hackers when sold on the Black Market. This is more than enough reason for a hacker to try to access your network.

When your business's network faces a data breach, you need a lifeline to hold onto. This is what Total Networks's Backup and Disaster Recovery (BDR) solution

accomplishes. In terms of recovery speed, you won't find a better resolution for your business's troubles. The BDR takes continuous snapshots of your data throughout the day, then sends them to an external data center for secure storage until they're needed. This means that your data is always up to date, which minimizes data loss in the event of a disaster.

Furthermore, the BDR solution enables rapid data recovery, which helps your business get back on its feet following a data breach. It does this by acting as your server in the event of a data breach or hardware failure. Your data is restored to the device, which temporarily resolves your downtime issues while you decide on a fix for your server woes. For more information about how your business can protect itself from data theft and loss, give Total Networks a call at (602)412-5025.



Share this Article!  
<http://bit.ly/1M6e18W>

## If Only Managed IT Service Extended to Your Car



Fact: Every piece of equipment requires maintenance on some level. The more intricate the equipment,

the more maintenance that's required. For enterprise-level computer networking equipment, maintenance can be outsourced and done remotely. Wouldn't it be great if this kind of service was available to other pieces of equipment that you use every day?

For example, consider your vehicle. It's an expensive machine that needs constant maintenance. Unless you happen to be a skilled mechanic, most consumers approach vehicle maintenance with a

break-fix approach; when the car breaks down, it's taken to the shop for a fix. As you may well know, this break-fix approach leads to hefty, unexpected repair bills, and of course, breakdowns happen at the worst possible times.

Generally speaking, the reason why maintenance is performed applies to both cars and computers; it keeps the equipment in tip-top shape. A piece of machinery in excellent condition will operate at maximum efficiency and will have far fewer breakdowns. On the contrary, by skipping out on maintenances, the probability of a major breakdown increases dramatically.

Therefore, if maintenance is the way to prevent such breakdowns, the next question to ask is, "How much maintenance must be done in order to circum-

vent these expensive repair jobs?" Answer: The more regular maintenance you can perform, the more reliable your equipment will be.

If we apply this principle to cars, we quickly see that there's a limitation to the amount of maintenance one can possibly perform. For example, cars can't be worked on while they're cruising down the highway, and it's not like you can change the engine oil while you're sleeping. But what if you could?

This is the idea behind managed IT service from Total Networks. We provide your company's IT network with 24/7 remote monitoring, and we're able to jump into action and remotely take care of an issue as soon as its spotted. This is in addition to performing regularly-

*(Continued on page 4)*

## Security Problems That Shape the Way Businesses View Cybersecurity in 2015

*(Continued from page 1)*

ate than your trusted IT department? They realize that you'll turn to them for help, and that you might willingly give away credentials to your IT department in order to access your infrastructure to perform "maintenance" or "resolve a critical issue." If you feel your IT department shouldn't be privy to certain information they are requesting, or if you receive suspicious emails from them concerning the integrity of your network, reach out to them via the phone number you have on record, rather than the one which might be in the email you've received.

### Hackers Won't Need Your Card to Scam You

Believe it or not, card-not-present (CNP) fraud is the real deal, and growing more

common. According to Verizon's 2015 PCI compliance report, payment fraud due to lost or stolen cards is decreasing, while fraud stemming from CNP situations only grows more prevalent.

These statistics reflect a shift in the manner through which hackers steal information (at least, in Canada it does). This change in tactics likely reflects hackers' adaptation to the increase in card security.

### VPNs Are Being Targeted

Some VPNs can be cracked if the hacker has access to sophisticated tools. One way this happens is when you use a VPN that only requires a username and password, rather than a more secure one which also uses two-factor authentication. It's recommended that you always

use two-factor authentication, especially when accessing corporate data through a mobile device.

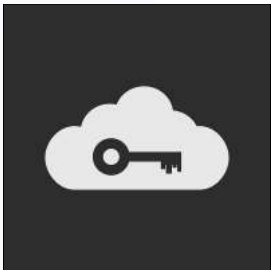
### Retail and Financial Hacks Are Growing More Common

Many big-box stores, like Target and Home Depot, have been hacked over the past year, and this trend will only continue in 2015. In fact, not too long ago, the IRS was hacked in an event which allowed hackers to access tax information for over 100,000 taxpayers. Businesses that take advantage of POS (point-of-sale) systems like cash registers and card readers will need to emphasize security and make it a top priority...



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

## 3 Ways Your Business Can Benefit from a Private Cloud Solution



Businesses are embracing the cloud model as the accepted form of computing, but some are finding that

they want more control over their data. When you use a public cloud, you're relinquishing some control so that you don't have to deal with network security and hosting. If you're serious about protecting your data and maintaining the infrastructure yourself, there are several benefits of operating your own private cloud infrastructure.

Of course, you need to ask yourself if the private cloud is the right computing solution for your business. It largely depends on how much control and responsibility you want placed on your shoulders. Businesses who prefer a hands-off approach to their technology will find that the public cloud is better suited to their needs, while those who want to have more control over their data will opt for the private cloud.

You don't want to jump into a private cloud project without knowing what you're getting yourself into. There are many factors that need to be considered before switching from a public to a private cloud, including new software, hardware, and network restraints. At the very least, your private cloud will need a virtual machine with a network that can back it up, as well as cloud computing software to distribute your applications and data throughout your infrastructure.

Here are three primary benefits of integrating a private cloud computing solution to your business model:

- **Enhanced Security Possibilities:** Security is always an important goal to shoot for when integrating a cloud solution, but when you're looking to integrate a private cloud infrastructure, it's essential. Normally, the cloud service's provider would handle the security measures in a public cloud setting; but in the case of the private cloud, it's up to the business to protect their data. This can be both a positive and negative aspect of the private cloud, as it presents the ability

to either ignore or augment your cloud's security with external solutions.

- **Greater Control:** As previously mentioned, you're in control when you decide to integrate a private cloud solution. This means that you're in charge of hosting and maintaining your cloud server. This might not sound like a benefit, but beneath the surface, you have greater access to data and admin settings than you would if you were using the public cloud.
- **Customization:** Many cloud vendors will give you several options for hosting on a public cloud, but when you host your own cloud server, you can integrate it your way. Choose which applications your team has access to, how much drive space is available for each of them, and of course, how much you want to invest into it.



Share this Article!  
<http://bit.ly/1M6fDPS>



## If Only Managed IT Service Extended to Your Car

(Continued from page 2)

scheduled maintenances, like installing security patches and upgrading software. This managed approach prevents issues from becoming problems that turn into expensive breakdowns. As far as maintenance goes, this level of equipment care is unprecedented.

Think what it would look like if your car received managed maintenance service that included 24/7 oversight. In order to pull this off, a licensed mechanic would have to show up at your home and work on your car while you sleep. Despite the fact that power tools would keep you from getting a good night's rest, your car would be working at optimal efficiency for your morning commute. And here's the best

part; you would never again have to worry about your car breaking down!

Additionally, when you're driving down the highway in a car that has managed maintenance service, the car would be uplinked to your mechanic's computer. This would allow him to monitor the vehicle's performance, and even make adjustments to the car's settings so that it gets maximum power and fuel economy.

Obviously, a managed-car maintenance service like this is too good to be true. However, what makes managed IT service so attractive to SMBs is that it provides this kind of comprehensive maintenance at an affordable rate. With

our managed IT service, computers are remotely worked on after-hours and our team of IT technicians monitor your equipment 24/7 for errors and potential threats.

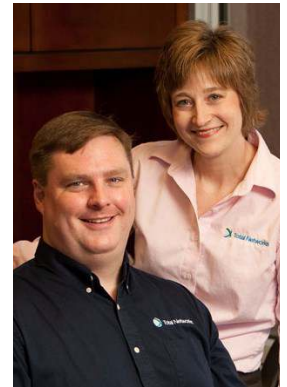
One benefit to this approach to computer maintenance is that your staff will come to work each morning and have access to workstations that are fine-tuned and error free. This allows your business to operate at maximum efficiency and minimizes the amount of downtime caused by preventable computer errors. To learn more about this revolutionary approach to computer maintenance, give Total Networks a call at (602)412-5025.



Share this Article!  
<http://bit.ly/1M6eqbw>

We work together with our IT Managed Services clients to jointly create and maintain an up-to-date, effective written technology plan and budget.

If you would like to receive an electronic version of our newsletter please email [skinsey@totalnetworks.com](mailto:skinsey@totalnetworks.com)



Dave and Stephanie Kinsey  
Owners

## How to Properly Store a Hard Drive



What's the best way to preserve your im-

portant files for years to come? Questions like this are being asked more frequently in our data-driven society. Here are some best practices when it comes to long-term data storage.

Let's say that you've got a hard drive full of pictures that are valuable enough to hold on to, but not worth storing on your primary computer. One common solution is to transfer the files to an external hard drive, or leave them on the hard drive of the old computer when it comes time to upgrade to a new one. These drives can then be stored away in a climate-controlled environment so they are available for future use.

For the average consumer, a data storage system like this creates a closet full of beige computers. Perhaps this describes your current data storage system, with each computer being referred to by the corresponding period of your life, like "my wedding computer," "my college computer," "my Disney vacation..."



Read the Rest Online!  
<http://bit.ly/1M6hVPb>



Bill Fox  
VP, Customer Service

## Total Networks

4201 North 24th Street  
Suite 230  
Phoenix, AZ 85016  
Voice: 602-412-5025

Visit us **online** at:  
[totalnetworks.com](http://totalnetworks.com)

-  [info@totalnetworks.com](mailto:info@totalnetworks.com)
-  [facebook.totalnetworks.com](https://facebook.totalnetworks.com)
-  [linkedin.totalnetworks.com](https://linkedin.totalnetworks.com)
-  [twitter.totalnetworks.com](https://twitter.totalnetworks.com)

