...for IT ingenuity

June 2012

The Intercom

A Monthly Newsletter of Invisik Corporation

Summer Greetings from Invisik!

Matt Jurcich, President
Invisik Corporation

Hello, Summer! Show of hands, everyone, if you've been cranking up the AC dial. Don't forget to frequently check and regulate the temperature in your server rooms, too. Now is also a good time to check-up on battery-backups, wires, and cords. Hot weather can wreak havoc on computers and peripherals running 24/7, and pro-active measures can go along way. Always feel free to give us a call if you find anything amiss.

June is also a great time to revisit IT project plans and goals. Give us a call if you have IT To Do items you hope to accomplish by year-end. Our vendor partners always have great hardware/software promotions happening, and they may just have what you've been waiting for. Give us a call at 612.298.3000 or email support@invisik.com.

Good networking,

Matt Jurcich

This Month...

WWW.INVISIK.COM
TEL: 612.298.3000 • EMAIL: SUPPORT@INVISIK.COM

Are FDIC Laws Enough to Protect Your Business from Cyber Thieves?

Here is an important question about your finances with a shocking answer: If a cyber-criminal were to gain access to your company's bank account and steal all of the money in it, could you get it back? In many cases, the answer is *no.*

Many small business owners falsely believe they are protected by Federal Deposit Insurance Corporation (FDIC) laws and that the bank (or Federal government) would replace money stolen by a thief. Not so. The FDIC protects bank accounts against *bank failures*, not theft or embezzlement. So if your money is taken by a criminal—be it a completely anonymous person or even a "trusted" employee or vendor—the bank is not responsible for replacing the funds.

What is really concerning about this is the fact that online criminals are becoming more and more sophisticated in their attacks. Criminals are also targeting small businesses since they are the "low hanging fruit"—small businesses often don't have the security systems in place to prevent these attacks. So what can you do to protect your business?

Keep Your Network SECURE!
Hackers are focusing on small business computer networks because they are far easier to crack than a bank's network. Weak passwords, out-of-date anti-virus, security patches that are not updated, and unmanaged firewalls are the simple security checks that hackers are counting on you to neglect. Don't be an easy target! At a minimum you should consider deploying a network monitoring system to help manage the security of key components of your IT infrastructure.

Educate Your Staff
While up-to-date anti-virus will protect you against a LOT of threats, it's not 100% effective in protecting you because the most common way criminals access financial accounts is through e-mail. Phishing scams, malware attachments in documents or links, or brute-force password guessing/reset attacks are examples of tricks these thieves use. The first two are usually successful because of user error—that is, employees or trusted account holders *give* hackers access by accidentally downloading malware, typing passwords in an e-mail, clicking on a link in an e-mail they believe to be safe, and so on. Therefore, it is imperative that anyone in your company authorized to access financial data and records should know NOT to click on strange links, open questionable attachments, or send any account information via e-mail.

Work with Your Bank
Find out exactly what their policy is for fraud, and what you can do to prevent problems. Some businesses have their bank set up "dual controls" on their account so that each transaction requires the approval of two people. Consider establishing a daily limit on how much money can be transferred out of your account, and even require that all transfers be prescheduled by phone or confirmed via phone call or text message. If possible, impose restrictions on adding new payees.

Watch Your Account Daily
You should also get into the habit of checking your accounts daily at the end of the day and notifying your bank immediately of any questionable withdrawals. Money is laundered quickly, so the sooner you catch the mistakes, the better your chances are of recovering the funds.

Make Sure Your Accountant Has Proper Security Controls
If you have someone doing your payroll and/or accounting, make sure they are following the same strict security procedures of your own computer network. Many hackers gain access through an authorized third party's PC—like a bookkeeper or accountant—and their credentials to clean out your account. It is essential that any and every employee, vendor or person accessing your financial accounts is following even tighter security controls on their PCs or other devices used to log into your bank, credit card accounts, or financial records.

If you have doubts about the security of your network or want more information about protecting your IT infrastructure, we are here to help. Contact us at 612.298.3000 or support@invisik.com for a consultation on industry leading tools to protect your business. ▲

Cloud-Speak that Floats You Away

Cloud computing systems are continuing to grow and become more popular, especially with small businesses. As cloud services continue to grow and evolve along with the needs of users and clients, the IT industry is primed for more positive developments in cloud services.

With new technology also comes new terminology—or, to many, just new technobabble. If you are feeling a bit "cloudy" about all the new Cloud-speak, we can help. Below are 10 of the most common cloud terms:

- **Cloud.** Cloud is the general term applied to anything that uses the Internet to provide an end user (in most cases, you) a service. Your information is hosted on a company's servers and is accessed via an Internet connection. Another way to think of it is like ordering delivery from a restaurant. For example, say you are in the mood for Italian food, but don't have the ingredients, so you have someone else do all the work and bring it to you.

- **Cloud OS (operating system).** A cloud operating system is an OS delivered via the Internet. The OS isn't physically on your system. It is located on a company's servers elsewhere, and you use a physical computer (at your office, home, or on wherever you are) to access it.

- **Cloud provider.** A company that provides a cloud service, storage, and servers (usually) for a fee.

- **Cloud storage.** A cloud service that allows users to store data off-site, and access it using the Internet.

- **Disruptive technology.** A technology that is so different and innovative it changes the way things are done. The cloud is a disruptive technology because it is changing the way business gets done.

- **Data center.** The physical building location where cloud servers are housed.

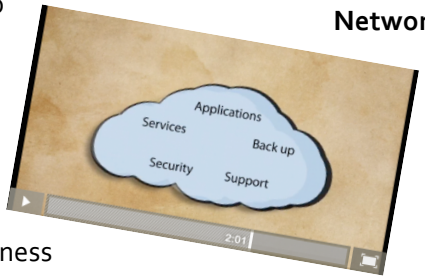
- **IaaS - Infrastructure as a Service.** This is the term used to describe any virtualized service being offered to a user. This can include virtualized servers, maintenance and software.

- **PaaS - Platform as a Service.** This term is used to describe any computing platform being offered over the Internet., It is typically the OS and related software.

- **SaaS - Software as a Service.** The term applied to a single piece of software that is offered over the Internet. Users access the software using the Internet instead of having to install it on their computer. Gmail is an example of a SaaS.

- **Client.** Despite what many believe, the client is not the person who buys a cloud service. The client is the device a user uses to access the cloud service. It could be a computer, laptop, tablet or even a smartphone.

These terms will give you a good start on navigating your way around cloud services as it continues to grow in popularity and usefulness. For a more detailed explanation of the benefits of cloud services, you can visit our website to download our FREE report **"5 Critical Facts Every Business Owner Must Know Before Moving Their Computer Network to the Cloud"** at www.invisik.com/cloudreport. Or catch our short video for a quick, but helpful illustration all about the cloud. View it at www.invisikcloudnetwork.com. For a no obligation Cloud Readiness Assessment contact us at 612.298.3000 or support@invisik.com. ▲



Invisik Trivia Bowl

June's Trivia Bowl Question:

In the northern hemisphere, the day the sun's rays are directly overhead along the Tropic of Cancer is called what?

A. Summer Solstice
B. Winter Solstice
C. Global Warming

Be the first to respond with the correct answer to win an iTunes gift card. Call **612.298.3000** or email **trivia@invisik.com**.

Congratulations to Sandra Jennings of Eden Prairie. She was the first to correctly answer May's question:

Who created Mother's Day in 1908 to fulfill her mother's dream of having a day to celebrate all mothers? (B.) Anna Jarvis

Psssst... Remember Our "Everybody-Wins-Referral-Program"!

☑ Yes! Send me a **$25 Visa Gift Card** for *each* of my business colleagues I'm referring to Invisik. I'll tell my colleagues to expect your call so they can get 2 FREE hours of guaranteed, no-strings-attached Invisik tech support to use anyway they want (a $300 value).

My Name: _____

Company: _____ Title: _____

My Referrals

Name & Title: _____

Company: _____

Phone: _____

Email: _____

Ye Ole Fine Print

My referral is the owner or person in charge of IT for a company with 10 or more desktops and at least 1 server.

Name & Title: _____

Company: _____

Phone: _____

Email: _____

Mail: 7240 Grand Ave S., Richfield, MN 55423 • Fax: 612.243.1477
Tel: 612.298.3000 • Email: support@invisik.com • www.invisik.com

Smart Protection for Laptops on the Go

Sunny summer days means more of us will be out and about with our laptops. Just the other day I came home and found my wife in the backyard; laptop on her knees, our 3-year old at her feet heaping sand on them (on her feet—not her laptop!) If, like us, you have a laptop on the go, consider protecting it from theft with LoJack for Laptops.

The company that provides LoJack for Laptops—Absolute Software— is NOT the same company that provides the vehicle recovery service that most of us know about (they license the name). Instead, Absolute Software provides a similar service in the sense that they help users track, manage, secure and recover mobile computers and devices.

Once installed, LoJack for Laptops will allow you to geographically locate your lost or stolen laptop. It also allows you to issue a remote command to freeze your lost or stolen computer and/or create a customized message to display on your computer's screen to help someone who finds it return it to you. If you know that it has fallen into the wrong hands, you can remotely erase files on your computer. You can opt to delete all of your files, or just certain file types. The next time your laptop contacts the Monitoring Center, it receives the "delete" command and erases the files you selected. For more details, visit lojackforlaptops.com or contact us at 612.298.3000 and support@invisik.com. ▲

Tips for Budgeting IT Expenses

Usually mid-way through the fiscal year like we are now, many clients will request consultations to discuss IT projects—like upgrades or installations—that they want to complete either by the year's end or to budget for the up-coming year. Not surprisingly, the most common question in these discussions is "How should I properly budget for IT expenses?" The answer, of course, depends on a lot of variables, so there is no "one-size-fits-all" solution, but below are some general guidelines that can help:

Hardware Refresh. No one likes the cost of a network upgrade, but it IS necessary approximately once every 3 to 4 years. PCs and servers older than that tend to run slow, crash frequently and generally become more expensive to fix and support than to replace. Therefore, your budget should include an IT refresh of all equipment every 3 years to be on the safe side.

Maintenance. There is no "set it and forget it" when it comes to network maintenance. With cyber criminals becoming more sophisticated and aggressive, you MUST constantly monitor and update your network against cyber-attacks, malware, data loss, etc. Budgeting for these proactive measures will save you money *and* aggravation in the long run.

Data Backup. Another expense you must account for is backing up your data to an offsite location. Since all businesses generate MORE data year after year, the backup will grow. Start by assessing the growth of your data over the last couple of years to uncover a trend. From there, forecast those additional expenses going forward at the same rate.

Expansion. Another factor for your IT budget is upgrading software, line of business applications, CRM systems and accounting packages that can no longer support your growing company. As your company grows, systems, processes and data become more complex requiring more sophisticated software and systems. Make sure you are looking ahead year upon year, and properly budget for it.

To better manage their IT expenses, many of our clients choose a customized package for their desktops, servers or entire IT infrastructure. Invisik Care Packages are a budget-friendly way to be proactive about taking care of important security and maintenance needs of your network. For a fixed monthly fee, different packages can include remote tech support, offsite backup and data recovery, managing security updates, and system-wide monitoring to catch potential issues before they bring your network down. We also have telephone and printer packages to significantly streamline your operations. Call 612.298.3000 or email support@invisik.com for details on a customized package for your business. ▲

The Smart Money is on Protecting Your Kids Online

In many homes across America, Summer Vacation heralds an increase of Internet usage by kids—supervised or not. Protecting them from inappropriate content online should not be a seasonal thing, of course, but if you have not yet installed parental controls to protect your children from harmful online risks, then now is as good a time as ever to start.

ContentWatch's Net Nanny Internet filter software ($39.99/yr at www.netnanny.com) helps you do just that. Parents find the software's following four features very useful:

1. Blocks "Mature" Games. The software scans the online game for its ESRB ratings (like movie ratings, but for computer games). If the game isn't kid-friendly, the computer blocks it.

2. Filters Facebook. Net Nanny can provide parents with a report on who their kids' "friends" are, what pictures and videos they are looking at, and their Facebook Instant Message conversations.

3. Prevents Proxy Sites From Working. Content filters work by making a "blacklist" of sites that it won't allow. If you tried to type in a blacklisted website address, you would not get very far. But there is a sneaky way around this called a "Proxy Server." Proxy Server web addresses are usually content neutral, so users can go there without flagging the blacklist system. Once in, your child can navigate to their original blacklisted site. Net Nanny prevents this by blocking both proxy server entries and the inappropriate website itself.

4. Keeps Parents Informed. Whenever your child is trying to gain access to something you have blocked, Net Nanny sends an e-mail notification to the parents.

Statistics report nearly 90% of 8-16 year olds have seen inappropriate images online. With frightening numbers of pornography, child predators, and other harmful online risks increasing, protecting your children's online activity is a MUST. For more information or help with content filters, contact us at 612.298.3000 or support@invisik.com ▲

More tech tips inside...

invisik corporation
7240 Grand Ave S
Richfield, MN 55423