TECHNOLOGY TIMES

Insider Tips To Make Your Business Run Faster, Easier, And More Profitably

By Computer Networks, Inc.

Serving Hampton Roads since 2004

Volume 8, Issue 6 June 2015

"As a business owner, you don't have time to waste on technical and operational issues. That's where we shine! Call us and put an end to your IT problems finally and forever!"

Rick Boyles, Owner/Founder
Computer Networks, Inc.

IT Guru, Published Author, and Trusted Advisor to Medical Practice Administrators and Business Owners

Hi, I am from the Internal Revenue Service and we are calling to tell you we have lost your Personally Identifiable Information…

You gotta be kidding me, right?

June 2, 2015
http://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application

The IRS announced today that criminals used taxpayer-specific data acquired from non-IRS sources to gain unauthorized access to information on approximately 100,000 tax accounts through IRS' "Get Transcript" application. This data included Social Security information, date of birth and street address.

See IRS Page 2

INSIDE THIS ISSUE

Does Your Cyberliability Insurance Carrier Love You?

Healthcare IT News
Erin Mcann

You had better hope so. Because it isn't working out too well for Cottage Health Systems in California. The three hospital group had a breach of 32,755 patients back in 2013 when one of their Vendors stored unencrypted ePHI on an Internet facing system.

A class action suit awarded the Plaintiffs $4.13 million. Cottage had a liability policy with Columbia Casualty Company who is now challenging the claims made by Cottage saying the Cottage Health folks "*provided false responses*" to a Security Risk self-assessment when it applied for the liability policy.

Columbia is alleging that Cottage failed to follow minimum required practices and as a result Columbia is not liable for paying the $4.13 million in awards.

Columbia further claims that Cottage failed to "regularly check and maintain security patches on its systems", failed "to regularly re-assess its information security exposure and enhance risk controls", failed "to have a system in place to detect unauthorized access or attempts to access sensitive information stored on its servers" and failed "to control and track all changes to its network" and that the Patient data breach occurred for those reasons.

See Liability Page 3

IRS continued from Page 1

These third parties gained sufficient information from an outside source before trying to access the IRS site, which allowed them to clear a multi-step authentication process, including several personal verification questions that typically are only known by the taxpayer. The matter is under review by the Treasury Inspector General for Tax Administration as well as the IRS' Criminal Investigation unit, and the "Get Transcript" application has been shut down temporarily. The IRS will provide free credit monitoring services for the approximately 100,000 taxpayers whose accounts were accessed. In total, the IRS has identified 200,000 total attempts to access data and will be notifying all of these taxpayers about the incident.

As always, the IRS takes the security of taxpayer data extremely seriously, and we are working aggressively to protect affected taxpayers and continue to strengthen our protocols.

Additional information

The IRS announced today it will be notifying taxpayers after third parties gained unauthorized access to information on about 100,000 accounts through the "Get Transcript" online application.

The IRS determined late last week that unusual activity had taken place on the application, which indicates that unauthorized third parties had access to some accounts on the transcript application. Following an initial review, it appears that access was gained to more than 100,000 accounts through the Get Transcript application.

In this sophisticated effort, third parties succeeded in clearing a multi-step authentication process that required prior personal knowledge about the taxpayer, including Social Security information, date of birth, tax filing status and street address before accessing IRS systems. The multi-layer process also requires an additional step, where applicants must correctly answer several personal identity verification questions that typically are only known by the taxpayer.

The IRS temporarily shut down the Get Transcript application last week after an initial assessment identified questionable attempts were detected on the system in mid-May. The online application will remain disabled until the IRS makes modifications and further strengthens security for it.

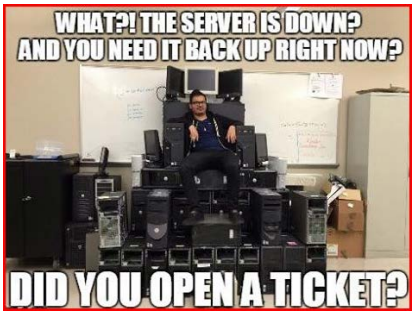
The matter is under continuing review by the Treasury Inspector General for Tax Administration and IRS offices, including Criminal Investigation.

The IRS notes this issue does not involve its main computer system that handles tax filing submission; that system remains secure.

On the Get Transcript application, a further review by the IRS identified that these attempts were quite complex in nature and appear to have started in February and ran through mid-May. In all, about 200,000 attempts were made from questionable email domains, with more than 100,000 of those attempts successfully clearing authentication hurdles. During this filing season, taxpayers successfully and safely downloaded a total of approximately 23 million transcripts.

The Get Transcript program has been shut down.❖

IT Throne



Predictable Results For a Predictable Fee

We do it all…HIPAA Security Risk Analysis, Backup and Disaster Recovery (required for HIPAA Compliance), Network Administration, Help Desk, Hardware Sales/Service, Hardware Refreshes/Installs, IT Consulting.

And, we do that for businesses with as few as 10 PCs.

We are looking for a select number of new clients in the medical and professional services fields.

If you are dissatisfied with the level of service you are getting from your current IT Vendor, pick up the phone, call me, Rick Boyles, at 757-333-3299 x200, or email me: rick.boyles@computernetworksinc.com and let's chat a bit about your needs. ❖

How To Make Yourself 'Invisible' To Hackers

There's an old joke about two men hiking in the woods when they come across a big, grumpy black bear. Scared silly, one of the guys starts to run but notices his buddy stopped, bent-over, changing his shoes. He shouts to him, "Dude! What are you doing?!?! Why aren't you running?" to which his friend replies, "I'm changing my shoes because I don't need to outrun the bear – I only need to outrun YOU."

This is a perfect analogy for what's going on in small businesses: the "slow," easy targets are getting nailed by fast-growing cybercrime rings that are getting more sophisticated and aggressive in attacking small businesses. Last year, the average cyber-attack cost a small business $20,752, a substantial increase from 2013, when the average was $8,699. That's because most small businesses don't have the security protocols in place or the manpower and budget to implement sophisticated security systems. While there's absolutely no way to completely protect yourself other than disconnecting entirely from the Internet, there are several things you can do to avoid being easy pickings. Here's how:

1. **Lock your wireless network.** While WIRED networks make you invisible to WiFi snoops because in order to connect you have to plug in a cable, you can create a hidden or cloaked network on a wireless network. Simply disable the service set identifier (SSID) broadcasting function on the wireless router, and only users with the exact network name will have access.
2. **Encrypt your data.** Purchasing a full-disk (hard drive) encryption software and enabling it keeps your info secure in the event of loss of the device.
3. **Install firewall and anti-malware applications** on all of your equipment, including mobile devices.
4. **Disable features that automatically connect your mobile devices to any available network.**
5. **Disable printer and file-sharing options on mobile devices before connecting to a hotspot.**
6. **Check before connecting to hotspots.** If there is an unusual variation in the logo or name on the login page, beware…this could mean it's a fake hotspot designed to steal your data.

Can you guarantee that the person across the hotel lobby isn't looking at your data? Not really, but the chances of them being able to do that are greatly reduced if you take precautions to protect your business. ❖

Liability continued from Page 1

In its application for the liability policy, Cottage Health System made "misrepresentations" regarding its security practices, and as such, Columbia is seeking reimbursement from the health system for the full $4.13 million that it had paid to Cottage thus far, in addition to attorney fees and related expenses.

In part of the application, Cottage answered "yes" to performing due diligence on third-party vendors to ensure their safeguards of protecting data are adequate; auditing these vendors at least once per year and requiring these third-party vendors have "sufficient liquid assets or maintain enough insurance to cover their liability arising from a breach of privacy or confidentiality."

The vendor who contributed to the data breach, inSync, according to the complaint, does not have sufficient assets ***or insurance*** that covers the breach.

You have a copy of YOUR IT company's Certificate of Insurance, don't you?

Let us know if you want to chat more about how to protect your business. Heck, we might even take you to lunch on our dime. ❖

Rick Boyles
757-333-3299 x200
rick.boyles@computernetworksinc.com

"How shall I torture you today?
Put you on the rack? Boil you in oil?
Make you call a technical support line?"

The Lighter Side:

"My wife only has two complaints: nothing to wear and not enough closet space..."

A Kansas farm wife called the local phone company to report her telephone failed to ring when her friends called and that on the few occasions, when it did ring, her dog always moaned right before the phone rang.

The telephone repairman proceeded to the scene, curious to see this psychic dog or senile lady.

He climbed a telephone pole, hooked in his test set, and dialed the subscriber's house.
The phone didn't ring right away, but then the dog moaned and the telephone began to ring.

Climbing down from the pole, the telephone repairman found:

1. the dog was tied to the telephone system's ground wire with a steel chain and collar.
2. the wire connection to the ground rod was loose.
3. the dog was receiving 90 volts of signaling current when the number was called.
4. after a couple of jolts, the dog would start moaning and then urinate.
5. the wet ground would complete the circuit, thus causing the phone to ring.

Which demonstrates that some problems CAN be fixed by pissing and moaning.

Just thought you'd like to know.

Managed Services aka Network Admin

Managed Services is the IT industry buzzword for bundling together a group of tasks that are normally performed by Network Administrators and charging a monthly fee for them.

The monthly fee for service model allows you to predict your costs and it incentivizes the IT company to solve your problems permanently, because they make less money when you are logging a bunch of service calls.

Some companies also handle Hardware Maintenance, which means that they take responsibility for the printers, scanners, Access Points and other computer hardware in your office.

Here are two industry charts of things that Clients expect in a Managed Services agreement and factors driving the decisions to hire a Managed Service Provider:

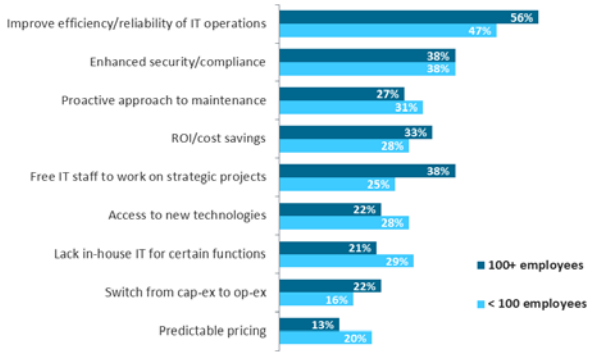
Managed Services by Type and Usage

	Nice to Have but Not Pay Extra	Nice to Have & Would Potentially Pay Extra	Expect as Part of Basic MSP Contract
Easy to read service level agreement	11%	23%	66%
Manage diverse range of devices, OSes, apps etc.	7%	26%	65%
Responsive/friendly customer service	12%	24%	64%
Near-perfect uptime	11%	26%	63%
East to understand predictable monthly pricing	11%	26%	63%
Detailed onboarding process for smooth transition	14%	23%	62%
Web-based dashboard	15%	26%	59%
Comprehensive reporting with usage metrics/analytics	15%	27%	58%
Advanced security safeguards	8%	35%	58%
Proactive maintenance and troubleshooting	5%	37%	58%
Single point of contact	19%	24%	57%
24/7 remote monitoring of systems, network etc.	9%	36%	56%
Expertise in a specific industry sector	17%	29%	55%
ROI calculator to gauge managed services	19%	29%	53%
Rapid response on-site service when needed	8%	40%	53%
Access to cutting-edge tech (cloud, mobility etc.)	12%	36%	52%

CompTIA

Source: CompTIA 4th Annual Managed Services Trends Study | Base: n=224 end-user businesses using managed services

Main Factors Driving End User Managed Services Decision



CompTIA

Source: CompTIA 4th Annual Managed Services Trends Study | Base: n=224 end-user businesses using managed services