

Your RMSCare Package

What's
Inside

\$1.5 Million
Cyber Heist

Page 2

Shiny New Gadget
of the Month

Nintendo
Classic

Page 3

3 "Must-Do"
Resolutions

Cont.

Page 3



Happy New Year! Or maybe I need to say Happy Thanksgiving, Merry Christmas and Happy New Year! We have been super busy the last few months, (and believe me I'm not complaining), as we have new clients, client moves, and client upgrades, but I have not published a newsletter in several months. I would say this is my New Year's Resolution to get them out every month but my clients IT needs do come first and I know that my track record with resolutions is not the best!! Speaking of resolutions, check out our Must Do IT Resolutions below!

I do hope all of you have had a wonderful holiday season and are ready for an even better 2017!

3 "Must-Do" IT Resolutions

Never before in the history of humankind have people across the world been subjected to extortion on a massive scale as they are today." That's what *The Evolution of Ransomware*, a study by Mountain View, California-based cybersecurity firm Symantec, reported recently.

If you have any illusions that your company is safe from cyber-attack in 2017, consider just a few findings stated in a recent report by the Herjavec Group, a global information security firm:

- Every second, 12 people online become a victim of cybercrime, totalling more than 1 million victims around the world every day.
- Nearly half of all cyber-attacks globally last year were committed against small businesses.
- Ransomware attacks rose more than an astonishing 300% in 2016.
- The world's cyber-attack surface will grow an order of magnitude larger between now and 2021.
- The US has declared a national emergency to deal with the cyberthreat.
- There is no effective law enforcement for financial cybercrime today.



Clearly, your company's information and financial well-being are at greater risk than ever in 2017. And you cannot count on the federal or state government or local police to protect your interests. That's why I STRONGLY SUGGEST that you implement the following resolutions starting TODAY.

Resolution #1: Tune up your backup and recovery system. The #1 antidote to a ransomware attack is an up-to-date backup copy of all your data and software. Yet managing backups takes more than just storing a daily copy of your data. For one thing, if your business is at all typical, the amount of data you store grows by 35% or more PER YEAR. If your data management budget doesn't expand likewise, expect trouble.

Cont. on Page 3

Don't Let This Happen To You!

\$1.5M Cyber-Heist Typifies Growing Threat

Efficient Escrow of California was forced to close its doors and lay off its entire staff when cybercriminals nabbed \$1.5 million from its bank account. The thieves gained access to the escrow company's bank data using a form of "Trojan horse" malware. Once the hackers broke in, they wired \$432,215 from the firm's bank to an account in Moscow. That was followed by two more transfers totaling \$1.1 million, this time to banks in Heilongjiang Province in China, near the Russian border. The company recovered the first transfer, but not the next two. They were shocked to discover that, unlike with consumer accounts, banks are under no obligation to recoup losses in a cybertheft against a commercial account. That meant a loss of \$1.1 million, in a year when they expected to clear less than half that. Unable to replace the funds, they were shut down by state regulators just three days after reporting the loss. Net result? The two brothers who owned the firm lost their nine-person staff and faced mounting attorneys' fees nearing the total amount of the funds recovered, with no immediate way to return their customers' money.

Avoid Getting Blindsided

While hacks against the big boys like Target, Home Depot and Sony get more than their share of public attention, cyber-attacks on small and medium-sized companies often go unreported, and rarely make national headlines.

Don't let this lull you into a false sense of security. The number of crippling attacks against everyday businesses is growing. Cybersecurity company Symantec reports, for example, that 52.4% of "phishing" attacks last December were against SMEs – with a massive spike in November. Here are just a few examples out of thousands that you'll probably never hear about:

Green Ford Sales, a car dealership in Kansas, lost \$23,000 when hackers broke into their network and swiped bank account info. They added nine fake employees to the company payroll in less than 24 hours and paid them a total of \$63,000 before the company caught on. Only some of the transfers could be canceled in time.

Wright Hotels, a real estate development firm, had \$1 million drained from their bank account after thieves gained access to a company e-mail account. Information gleaned from e-mails allowed the thieves to impersonate the owner and convince the bookkeeper to wire money to an account in China.

Maine-based PATCO Construction lost \$588,000 in a Trojan horse cyber-heist. They managed to reclaim some of it, but that was offset by interest on thousands of dollars in overdraft loans from their bank.

Why You're A Target – And How To Fight Back!

Increasingly, cyberthieves view SMEs like yours and mine as easy "soft targets." That's because all too often we have:

1. Bank accounts with thousands of dollars.
2. A false sense of security about not being targeted.
3. Our customers' credit card information, social security numbers and other vital data that hackers can easily sell on the black market.

If you don't want your company to become yet another statistic in today's cyberwar against smaller companies, and your business doesn't currently have a "bullet-proof" security shield, **you MUST take action without delay – or put everything you've worked for at risk. The choice is yours.**

Here are three things you can do right away:

1. Remove software that you don't need from any systems linked to your bank account.
2. Make sure everyone with a device in your network NEVER opens an attachment in an unexpected e-mail.
3. Require two people to sign off on every transaction.

Let Us Help

When it comes to defending your data, whether it's bank account information, customer and employee records or proprietary intellectual property or processes, Do NOT take chances. Our experience and track record in keeping our clients' data safe speaks for itself:

Shiny New Gadget Of The Month:



New Nintendo Classic Rules Them All!

For anyone in their late 20s to early 40s, chances are nothing shaped your life more than Nintendo. If it was your first “gadget,” it may even have been love at first sight.

And now, for Nintendo lovers, the Nintendo Entertainment System is back and better than ever with the NES Classic Edition. It’s tiny, but designed to look just like the original NES. Setup is a snap. Just plug it into your TV’s USB port. Hit the power button and you’re greeted with a screen where you can browse games and options. You can even select a CRT filter that replicates the lines and look of an old TV.

The color is sharp, the timing dead on and each pixel is a perfect square so you see the games exactly as designed. At 60 bucks, it’s a great gift for your favorite millennial (maybe even YOU!).

3 “Must-Do” IT Resolutions For 2017

Cont. from Page 1

Resolution #2: Harness the power of the cloud—but watch your back. Huge productivity gains and reduced costs can be achieved by making full use of the cloud. Yet it’s a double-edged sword. Any oversight in security practices can lead to a breach. Here are two things you can do to harness the cloud safely:

- *Determine which data matters.* Some data sets are more crucial to your business than others. Prioritize what must be protected. Trying to protect everything can take focus and resources away from protecting data such as bank account information, customer data and information that must be handled with compliance and regulatory requirements in mind.
- *Select cloud providers carefully.* Cloud vendors know that data security is vital to your business and promote that fact. Yet not all cloud vendors are the same. You can’t control what happens to your data once it’s in the cloud, but you can control who’s managing it for you.

Resolution #3: Set and enforce a strict Mobile Device Policy. As BYOD becomes the norm, mobile devices open gaping holes in your network’s defenses. Don’t miss any of these three crucial steps:

Require that users agree with acceptable-use terms before connecting to your network. Be sure to include terms like required use of hard-to-crack passwords, conditions under which company data may be “wiped” and auto-locking after periods of inactivity.

Install a Mobile Device Management System on all connected devices. A good system creates a virtual wall between personal and company data. It lets you impose security measures, and it protects user privacy by limiting company access to work data only.

Establish a strong protocol for when a connected device is lost or stolen. Make sure features that allow device owners to locate, lock or wipe (destroy) all data on the phone are pre-set in advance. That way, the user can be instructed to follow your protocol when their phone is lost or stolen.

Free Network And Security Audit Resolves Your Biggest Data Security Problems and Makes Your Systems Run Like A Fancy Swiss Watch

Ever asked yourself why some business owners and CEOs seem so blithely unconcerned about data protection? Don’t let their ignorance lull you into a false sense of security. If you’ve read this far, you are smart enough to be concerned.

Call us right now at 770-988-9640 and we’ll send one of our top network security experts over for a FREE Network and Security Audit. It’s your best first step to a safe and prosperous 2017.

RMS Associates, Inc.

1850 Lake Park Drive
Suite 200
Smyrna, GA 30080
www.rmsatl.com
Phone: 770.988.9640
Fax: 770.988.9695



Services We Offer

- ◆ Cloud Solutions
- ◆ Technology as a Service
- ◆ Total Business Continuity Protection
- ◆ Proactive Network Maintenance/Monitoring
- ◆ Network Design & Implementation
- ◆ Network Security
- ◆ SPAM & Virus Remediation & Prevention
- ◆ 3CX VOIP Phone System



Bring on the New Year!!

Happy 2017!

“Like” RMS Associates, Inc. on FaceBook to get the latest IT news, tips, and even an occasional laugh at facebook.com/RMSAssociates



Check out our blog at mysupportguys.com/blog

Subscribe to our RSS feed at mysupportguys.com/feed.



Yes, I put on some weight during the holidays but no worries, it's mostly water!

We Would Love To Hear From YOU!

If you have noticed an RMS associate going above and beyond the ordinary for you either on-site or over the phone, please let us know so we may reward them! Please e-mail me at rrowe@rmsatl.com. Thanks!

This newsletter is printed by Imagers, a long time client and friend. If you need quality specialized printing, please call them at 404-351-5800 or see them on the web at www.imagers.com.

