ONIT Technology Solutions

When You Fall Victim To A Cybercrime Attack Through No Fault Of Your Own, Will They Call You

Stupid…Or Just Irresponsible?

An URGENT Notice To All Non-Profit Administrators and CEOs In San Antonio:

We have entirely FREE and time-sensitive information that is critical for you as an administrator or CEO to know regarding growing cyber security threats AND your organization's credentials being sold on the "Dark Web." **Please respond ASAP.**

February 14, 2020
From The Desk of: Jay Guerra
CEO, ONIT Technology Solutions

Dear Colleague,

It's EXTREMELY unfair, isn't it? Victims of all other crimes – burglary, mugging, carjacking, theft – get sympathy from others. They are called "victims" and support comes flooding in, as it should.

But if your institution is the victim of a cybercrime attack where the benefactor or donor data is stolen or accessed, you will NOT get such sympathy. You will be instantly labeled as stupid or irresponsible. **You will be investigated and questioned about what you did to prevent this from happening** – and if the answer is not adequate, you can be found liable, facing serious fines and lawsuits EVEN IF you trusted an outsourced IT support company to protect you.

Claiming ignorance is not an acceptable defense, and this giant, expensive and reputation-destroying nightmare will land squarely on YOUR shoulders. *But it doesn't end there…*

According to current data protection laws, you will be required to tell your donors, clients and patients that YOU exposed them to cybercriminals. They will be IRATE and leave in droves. Morale will TANK and employees will BLAME YOU. Your bank is NOT required to replace funds stolen due to cybercrime (*go ask them*), and unless you have a very specific type of insurance policy, any financial losses will be denied coverage.

Please do NOT underestimate the importance and likelihood of these threats. It is NOT safe to assume the company you are outsourcing your IT support to is doing everything they should be doing to protect you; in fact, **there is a high probability they are NOT, which is**

why we're writing you today…

Why We Want To Offer You A FREE Cyber Security Risk Assessment

My name is Jay, CEO of ONIT Technology Solutions. We specialize in being the outsourced IT department for organizations like yours in the San Antonio area since 2012.

Over the last year, I've seen a significant increase in calls from administrators and CEOs desperate for help after a ransomware attack, data breach event or other cybercrime incident.

What makes this unforgivable is that they ALL had an IT company they trusted with the responsibility of protecting the organization, but realized all too late the company wasn't doing the job it was PAID to do.

Because this has become an all-too-common event, we're offering a FREE Cyber Security Risk Assessment to institutions in our area to reveal if your current security and backup systems are sufficient to protect you from a cyber-attack.

After all, if your operation was vulnerable to a cyberthreat, wouldn't you want to know?

The Answers You Want, The Certainty You Need

Here's How It Works: At no cost or obligation, one of my lead consultants and I will come to your office and conduct a non-invasive, CONFIDENTIAL investigation of your computer network, backups and security protocols. Your current IT company or guy does not need to know we are conducting this assessment; however, we would hope they'd openly welcome a set of "fresh eyes" on what they're doing.

Your time investment is minimal: one hour for the initial meeting and one hour in the second meeting to go over our Report Of Findings.

When this Risk Assessment is complete, you will know:

- **If your e-mail address and login credentials are being exposed on the Dark Web** (I can practically guarantee one or more are… THIS will shock you). Thanks to a new threat-intelligence and monitoring service, we can run a report on YOUR organization's e-mail addresses and see which ones are actively exposed on the Dark Web, which is a part of the World Wide Web accessible only by means of special software, allowing operators to remain completely and totally anonymous and untraceable, used by the most notorious cybercrime rings around the world.

- **IF your IT systems and benefactor & donor data are truly secured from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees.** *If you're not getting weekly security updates from your current IT person, your systems probably aren't secure.* You should also know that antivirus software and most firewalls are grossly inadequate against the sophisticated attacks now happening.

- **IF your current backup would allow you to be back up and running again fast if ransomware locked all your files.** *In 99% of the computer networks we've reviewed over the years, the administrators were shocked to learn the backup they had would NOT survive a ransomware attack*. Ransomware is **designed to infect your backups as well**, leaving you defenseless. There are only a handful of backup systems that will prevent this from happening.

- **IF your IT systems, backups, policies and procedures meet compliance requirements** for [HIPAA/GLBA/SOX/PCI]. The laws are expanding and getting more strict regarding data privacy for ALL businesses. This is an area you do not want to overlook – and you might be violating one or more data-protection laws without knowing it.

If we DO find problems – overlooked security loopholes, inadequate backups, credentials that have been compromised, out-of-date firewall and antivirus software and (often) active malware – on one or more of the PCs in your office, we will propose an Action Plan to remediate the situation that you can have us implement for you if you choose. **Again, I want to stress that EVERYTHING WE DISCUSS AND DISCOVER WILL BE STRICTLY CONFIDENTIAL.**

Why Free?

Frankly, we want the opportunity to be your IT company. We know we are the most competent, responsive and trusted IT services provider to small businesses in San Antonio.

However, I also realize **there's a good chance you've been burned, disappointed and frustrated by the complete lack of service and the questionable advice** you've gotten from other IT companies in the past. In fact, you might be so fed up and disgusted with being "sold" and underserved that you don't trust anyone. *I don't blame you*.

That's why this assessment is completely and entirely free. Let us earn your trust by demonstrating our expertise. While we would love the opportunity to be your IT company, we will come in with no expectations and only look to provide you with fact-based information so you can make a quality, informed decision – and we'll ONLY discuss the option of becoming your IT company if the information we share makes sense and you want to move forward. No hard sell. **No gimmicks and no tricks.**

Please…Do NOT Just Shrug This Off
(This Is A Limited Offer)

I know you are *extremely busy* and there is enormous temptation to discard this, shrug it off, worry about it "later" or dismiss it altogether.

That is, undoubtedly, the easy choice…but the easy choice is rarely the RIGHT choice. **This I can guarantee:** at some point, you WILL be forced to deal with a cyber "event."

Hopefully you'll be brilliantly prepared for it and experience only a minor inconvenience. But if you wait and do NOTHING, I can practically guarantee it will be a far more costly, disruptive and devastating attack that will happen to your non-profit business.

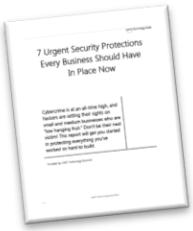
Schedule Your Free Risk Assessment By Going To:
www.123onit.com/secure

This is a LIMITED offer that will expire on: **March 6, 2020**

Don't "hope" your IT guy has you covered. **Get the facts and be certain you are protected.**

Dedicated to serving you,

Jay Guerra
Web: www.123onit.com
E-mail: jguerra@123onit.com
Direct: 210-263-3810



Not Ready To Meet Just Yet?

Then at least allow me to send you our free Executive Report titled **"7 Urgent Security Protections Every Business Should Have In Place Now."** This Executive Report is brief, concise and contains facts and information that might mean the difference between surviving this terrible and growing storm of cybercrime coming or being financially devastated and sunk. You can instantly download this report for free at www.123onit.com/security-report or you can call my office at 210-263-3810 for your free copy.

You can download it at www.123onit.com/security-report