# The 7 Most Critical IT Security Protections Every Business Must Have In Place NOW To Protect Themselves From Cybercrime, Data Breaches And Hacker Attacks

**Cybercrime is so widespread that it's practically inevitable that your business – large OR small – will be attacked. However, a few small preventative measures CAN PREPARE YOU and minimize (or outright eliminate) any reputational damages, losses, litigation, embarrassment and costs.**

Provided By: iTrust IT, LLC
Author: Scott Minke
9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177
www.iTrust-IT.com, 817.886.7966

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

# Stupid…Or Just Irresponsible?

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

**But if your business is the victim of a cybercrime attack where client or patient data is compromised, 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 (You'll learn the meaning of the term lawyers in those cases term: "Due Care")– and if the answer is not adequate, **you can be found liable**, facing serious fines and lawsuits. You will be required by law to tell your clients and/or patients that YOU exposed their private records, financials and data to criminals. **Your competition will have a heyday over this**, and **clients will leave in droves once they discover you've been compromised**. Your bank will NOT come to your rescue either, and unless you have a very specific type of crime insurance, **any financial losses will not be covered**.

## Here's The Ugly Truth:

You already know that cybercrime is a very real threat to you – but it's very possible that you're underestimating the potential damage posed by these threats.

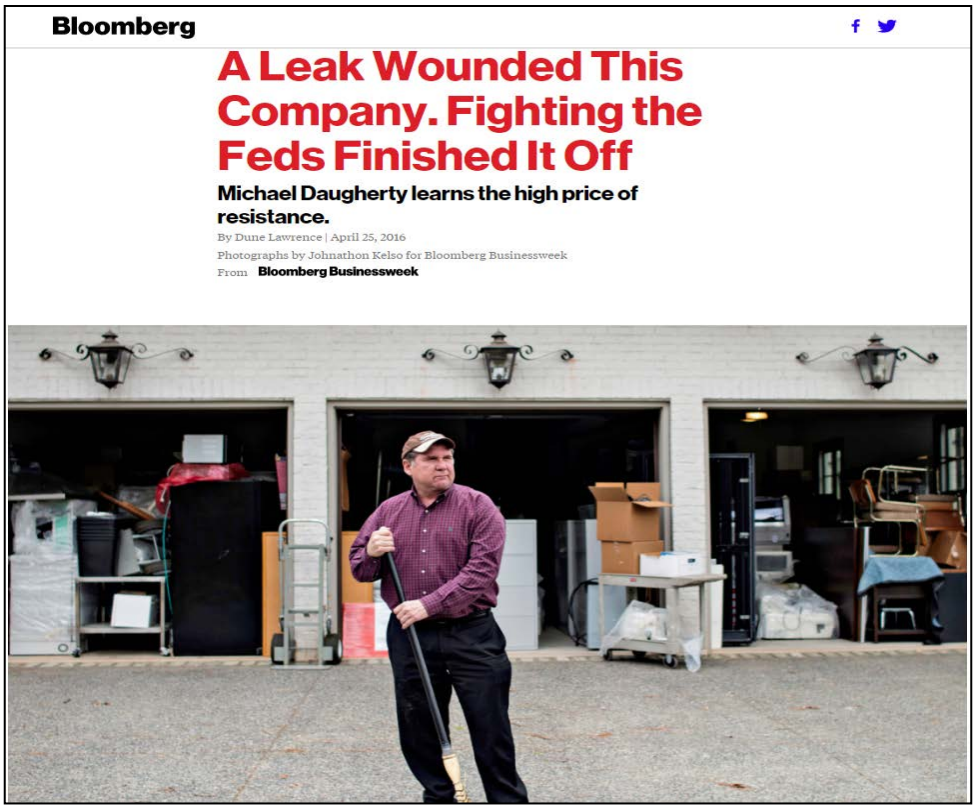
**ONE cyber-attack**…one slipup from even a smart, tenured employee clicking on the wrong e-mail…**can open the door to ABSOLUTE FINANCIAL DEVASTATION**, and undo everything you've worked so hard to achieve. **Take the story of Michael Daugherty, former CEO of LabMD.** His $4 million Atlanta-based company tested blood, urine and tissue samples for urologists – a business that was required to comply with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA.

He **HAD an IT team in place** that he **believed** was protecting them from a data breach – yet the manager of his billing department was able to download a file-sharing program to the company's network to listen to music, and unknowingly left her documents folder (which contained over 9,000 patient files) open for sharing with other users of the peer-to-peer network. This allowed **an unscrupulous IT services company**

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

to hack in and gain access to the file and use it against them for extortion. When Daugherty refused to pay them for their "services," the company **reported him to the Federal Trade Commission**, who then came knocking. After filing some 5,000 pages of documents to Washington, **he was told the information he had shared on the situation was "inadequate,"** and the **FTC requested in-person testimony from the staff regarding the breach**, and more **details on what training materials he had provided to his employees regarding cybersecurity**, **firewalls** and **security policies**. (QUESTION: ARE YOU ACTUALLY DOING ANY OF THIS NOW? WOULD YOU EVEN KNOW WHERE TO BEGIN?)

Long story short, **his employees blamed HIM and left**. **Sales steeply declined as clients took their business elsewhere**. **His insurance providers refused to renew their policies**. The emotional strain on him – not to mention the financial burden of having to pay attorneys – took its toll, and **eventually he closed the doors to his business**, jamming medical equipment into his garage where it remains today (image below).


Bloomberg

A Leak Wounded This Company. Fighting the Feds Finished It Off

Michael Daugherty learns the high price of resistance.

By Dune Lawrence | April 25, 2016

Photographs by Johnathon Kelso for Bloomberg Businessweek

From Bloomberg Businessweek

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

# "Not My Company…Not My People…" You Say?

**Don't think you're in danger because you're "small" and not a big target like a J.P. Morgan Chase or Home Depot? Or that you have "good" people and protections in place?** Think again. **Every single day, 978,000 NEW malware threats are being released**, and **more than HALF of the cyber-attacks occurring are aimed at small businesses**; you just don't hear about it because **it's kept quiet** for fear of attracting bad PR, lawsuits and data-breach fines, and **out of sheer embarrassment** – but make no mistake: small businesses are being compromised daily, and **the smug ignorance of "that won't happen to me" is an absolute surefire way to leave yourself wide open to these attacks.**

In fact, the National Cyber Security Alliance reports that **one in five small businesses have been victims of cybercrime in the last year** – and that number is growing rapidly as more businesses utilize cloud computing and mobile devices and store more information online.

You can't turn on the TV or read a newspaper without learning about the latest online data breach, and government fines and regulatory agencies are growing in number and severity. **Because of all of this, it's critical that you have these seven security measures in place.**

Many business owners are shocked when they get compromised because they BELIEVED they had it "handled." However, there is a virtual army of thousands of hackers and very sophisticated crime rings that work around the clock to overcome known protections – and **you can't stop a brand-new threat that was invented yesterday with a security system that was designed six months to a year ago**. It requires special expertise and training to stay on top of all of this, which is why many small businesses don't.

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

**To that end, here's your quick [7]-step checklist. If YOUR company isn't actually implementing ALL of these protocols – OR if you don't know if you are – WE CAN HELP. Read on!**

1. **The #1 Security Threat To ANY Business Is**…You and your employees! Like it or not, **almost all security breaches in business are due to an employee clicking, downloading or opening a file that's infected**, either on a website or in an e-mail; once a hacker gains entry, they use that person's e-mail and/or access to infect all the other PCs on the network. Phishing e-mails (an e-mail cleverly designed to look like a legitimate e-mail from a website or vendor you trust) are still a very common occurrence – and spam filtering and antivirus cannot protect your network if an employee is clicking on and downloading the virus. That's why **it's CRITICAL that you educate all of your employees in how to spot an infected e-mail or online scam**. Cybercriminals are EXTREMELY clever and can dupe even sophisticated computer users. All it takes is one slipup, so constantly reminding and educating your employees is critical.

   On that same theme, the **next precaution is implementing an Acceptable Use Policy**. An AUP outlines how employees are permitted to use company-owned PCs, devices, software, Internet access and e-mail. **We strongly recommend putting a policy in place that limits the websites employees can access with work devices and Internet connectivity**. Further, you have to enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what websites your employees access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others.

   **Having this type of policy is particularly important if your employees are using their own personal devices and home computers to access company e-mail and data**. With so many applications in the cloud, an employee can access a critical app from any device with a browser, which exposes you considerably.

   If an employee is logging in to critical company cloud apps through an infected or unprotected, unmonitored device, it can be a gateway for a hacker to enter YOUR network – which is why we don't recommend you allow employees to work remote or from home via their own personal devices.

   Second, if that employee leaves, are you allowed to erase company data from their phone or personal laptop? If their phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos, videos, texts, etc. – to **ensure YOUR clients' information isn't compromised**?

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

Further, if the data in your organization is highly sensitive, such as patient records, credit card information, financial information and the like, you may not be legally permitted to allow employees to access it on devices that are not secured, but that doesn't mean an employee might not innocently "take work home." If it's a company-owned device, you need to detail what an employee can or cannot do with that device, including "rooting" or "jailbreaking" the device to circumvent security mechanisms you put in place.

2. **Ask your current Business Insurance Carrier if you have sufficient "Cyber Liability" coverage.** All too often, Business owners are shocked to find that their current Insurance policy doesn't adequately cover Cyber-Crime. **Many insurance policies are conveniently vague in these areas as they lack the resources to understand how to properly write policies that cover businesses when cybercriminals strike them or their customers.** Though we don't sell insurance—we CAN direct you to trusted Insurance Advisors who can help you look at your current Insurance Policies as they relate to Cyber-Crime coverage. **The best time to have the conversation is NOW before you've been breached and your business hangs in the balance of whether or not you have coverage!**

3. **Keep your network and all devices patched and up-to-date.** New vulnerabilities are frequently found in common software programs you are using, such as Adobe, Flash, Microsoft or QuickTime; therefore **it's critical you patch and update your systems and applications when patches become available**. If you're under a managed IT plan, this is all automated for you so you don't have to worry about an employee missing an important update.

4. **Have A Business-Class Image Backup BOTH On-Premise And In The Cloud.** This **can foil the most aggressive (and new) ransomware attacks**, where a hacker locks up your files and holds them ransom until you pay a fee. If your files are backed up, you don't have to pay a crook to get them back. **A good backup will also protect you against an employee accidentally (or intentionally!) deleting or overwriting files, and against natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters**. Again, your backups should be AUTOMATED and monitored; the worst time to test your backup is when you desperately need it to work!

5. **Don't allow employees to access company data with personal devices that aren't monitored and secured by YOUR IT DEPARTMENT.** The use of personal and mobile devices in the workplace is exploding. Thanks to the

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

convenience of cloud computing, you and your employees can gain access to pretty much any type of company data remotely; all it takes is a known username and password. Employees are now even asking if they can bring their own personal devices to work (BYOD) and use their smartphone for just about everything.

But **this trend has DRASTICALLY increased the complexity of keeping a network – and your company data – secure**. In fact, your biggest danger with cloud computing is not that your cloud provider or hosting company will get breached (although that remains a possibility); the **biggest threat is that one of your employees accesses a critical cloud application via a personal device that is infected**, thereby giving a hacker access to your data and cloud application.

So **if you ARE going to let employees use personal devices and home PCs, you need to make sure those devices are properly secured, monitored and maintained by a security professional**. Further, do not allow employees to download unauthorized software or files. One of the fastest ways cybercriminals access networks is by duping unsuspecting users into willfully downloading malicious software by embedding it within downloadable files, games or other "innocent"-looking apps.

But here's the rub: **most employees won't want you monitoring and policing their personal devices**; nor will they like that you'll wipe their device of all files if it's lost or stolen. But that's exactly what you'll need to do to protect your company. Our suggestion is that you allow employees to access work-related files, cloud applications and e-mail only via company-owned devices and devices monitored and managed by your IT Department, and never allow employees to access these items on unmanaged personal devices and public WiFi.

6. **A Business-Class Good Firewall And Proper Updates.** A firewall **acts as the frontline defense against hackers**-- blocking everything you haven't specifically allowed to enter (or leave) your computer network. But **all firewalls need monitoring and maintenance**, just like all devices on your network, or they are completely useless. This too **should be done by your IT person or company as part of their regular, routine maintenance**.

7. **Protect Your Bank Account.** Did you know your COMPANY'S bank account **doesn't enjoy the same protections as a personal bank account**? For example, if a hacker takes money from your business account, the **bank is NOT responsible for getting your money back**. (Don't believe me? Go ask your bank what their policy is on refunding you money stolen from your account!) Many

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

**people think FDIC protects you from fraud**; it doesn't. It protects you from bank insolvency, NOT fraud.

So here are **three things you can do to protect your bank account**. First, **set up e-mail alerts on your account** so you are notified any time money is withdrawn. **The FASTER you catch fraudulent activity, the better your chances are of keeping your money**. In most cases, fraudulent activity caught the DAY it happens can be stopped. If you discover it even 24 hours later, you may be out of luck. That's why it's critical that you monitor it daily and contact the bank IMMEDIATELY if you see any suspicious activity.

**Second**, if you do online banking, **dedicate ONE computer to that activity** and **never access social media sites, free e-mail accounts (like Hotmail) and other online games, news sites, etc., with that PC.** Remove all bloatware (free programs like QuickTime, Adobe, etc.) and make sure that machine is monitored and maintained behind a strong firewall with up-to-date antivirus software.

And **finally**, **contact your bank about removing the ability for wire transfers out of your account** and **shut down any debit cards associated with that account**. All of these things will greatly improve the security of your accounts.

## Are You REALLY Willing To Be Complacent About This?

Look, I know **all of this appears to be a giant distraction and cost that interferes with REAL work**. You and I both realize that implementing proper security protocols won't win you the "employer of the year" award or deliver an ROI – in fact, we HOPE by doing OUR job, it never has to deliver one.

BUT **if you foolishly choose to turn a blind eye** and be arrogant, complacent or careless, **cybercriminals WILL take advantage of you**. **This tsunami of pain will land directly on YOUR desk to deal with, everyone pointing the blame at YOU**. YOUR bank account. YOUR business. You will be faced with significant losses, costs and an emotional drain on you and your team as you deal with a breach.

## Mark Twain Once Said, "Supposing Is Good, But KNOWING Is Better"

**If you are concerned about** employees and **the dangers of cybercriminals gaining access to your network**, then **take the first step** and call or email us so that

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

WE together can take the first step to implementing a **Managed Security Plan for your Business**—which starts from the Outside-In!

To start with-- We'll conduct a **FREE Dark Web Scan** (A $500 Value that's potentially invaluable) looking for any information associated with your company that is currently available to hackers. This information might include:

- **Usernames and Passwords to equipment WITHIN YOUR NETWORK.**
- **Administrative & other Login information to commonly-accessed websites that your staff accesses every day to do their jobs**
- **Corporate & Accounting Staff Names, Phone Numbers, Mobile Phone Numbers, and email addresses that would allow the hackers to impersonate you**
- **CLIENT/CUSTOMER Corporate & Accounting Staff Names, Phone Numbers, Mobile Phone Numbers, and email addresses that allow the hackers to IMPERSONATE your Clients/Customers and worse—to THEIR CLIENTS AND CUSTOMERS.**
- **PCI, HIPAA, SOX or other data-privacy law violations. New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines if that information is leaked.**
- **Intellectual Property & Proprietary Information that you'd NEVER want sold to the Highest Bidder or to your competition!**

**I know it's natural to want to think, "We've got it covered" or "This Will Never Happen to Us"** -- Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks & subsequent data loss and extended downtime – I just see it all too often in the daily news and it's **EXTREMELY RARE for us not to find anything truly-concerning on the Dark Web.** IF your company is the exception—then you will at least sleep better knowing that you exercised due care by having us perform the scan on your behalf.

It simply **never hurts to have us check to see what's been leaked on the Dark Web**.

I have no one to protect and no reason to conceal or gloss over anything we find. If you

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177

want the straight truth, I'll report it to you. **ALSO AND MOST-IMPORTANTLY – We will report our findings ONLY TO YOU—keeping the private results of your scan PRIVATE and SECURE.**

Dedicated to serving you,

**Scott Minke, Founding Partner/CEO**
**iTrust IT, LLC**

Web: www.iTrust-IT.com
E-mail: Scott@iTrust-IT.com

© 2018 iTrust IT, LLC – ALL RIGHTS RESERVED - www.iTrust-IT.com – 9800 Hillwood Pkwy. Ste 140, Fort Worth, TX 76177