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: Zanacore Technologies
Author: Jack Marder, CEO
625 Beaver Ruin Rd NW STE E
Lilburn, GA 30047

www.zanacore.com

678-822-5815

Zanacore TECHNOLOGIES

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 – 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:

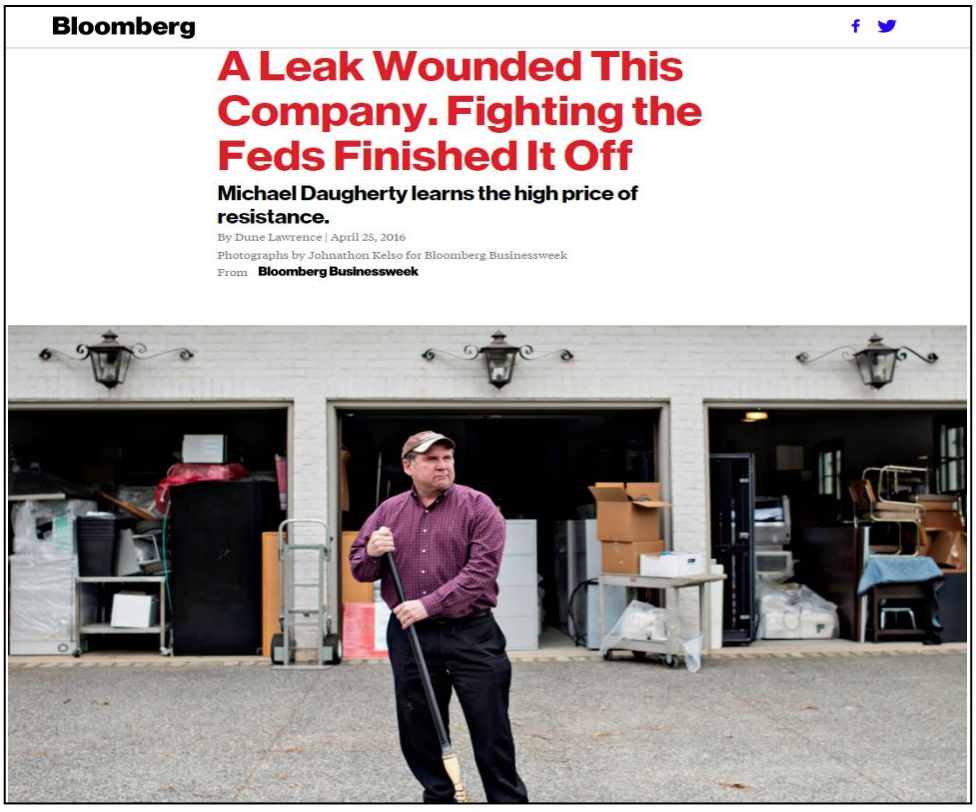
You already know that cybercrime is a very real threat to you – but it's very possible that you're underestimating the potential damage, OR **you are being ill-advised** and underserved by the employees and/or vendors you hired to protect your business from these threats.

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 a questionable IT security company to gain access to an exposed file and allegedly use it against them for extortion. When Daugherty refused to hire 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 manuals he had provided to his employees regarding cybersecurity, documentation on firewalls and penetration testing. (QUESTION: ARE YOU ACTUALLY DOING ANY OF THIS NOW?)

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).



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

Perhaps you don't think you're in danger because you're "small" and not a big target like a J.P. Morgan or Home Depot. Or that you have "good" people and protections in place? Think again. Every single day, 82,000 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 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.**

But I Have a Great IT Guy I Trust…

Many business owners are shocked when they get compromised because they BELIEVED their IT company or guy 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 to stay on top of all of this, which is why many don't.

To that end, here's your quick 7-step checklist. If YOUR company isn't implementing ALL these protocols – OR if you don't know if you are – WHY NOT? What hasn't your current IT company told you about all of this?

1. **Train Employees on Security Best Practices.** The #1 vulnerability for business networks are the employees using them. Most of the data breaches today are still caused by employees unknowingly clicking on dangerous links in e-mail. It's extremely common for an employee to infect an entire network by opening and clicking in a Phishing e-mail (that's an e-mail cleverly designed to look like a

legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network.

You need to have management buy-in on taking security seriously or it won't work in the rest of the organization. Train employees about company policies and the risk with mobile devices. Define what employees are allowed to do and prohibited from doing with business data and company computers. Teach them what Phishing schemes look like in e-mail messages so they can avoid unknowingly becoming a victim. The good news is that it's easy to train employees how to avoid becoming a victim of cybercrime. Your IT Vendor should help you do that.

2. **Require STRONG passwords and passcodes**. Strong passwords are absolutely critical for protecting your data, but amazingly, it's the one area I get the most push-back from my clients. If you only have a simple password, Cyber Criminals can hack into your account within milliseconds. But it would take days to hack an account with a strong and complex password and most would-be criminals give up long before then and move on to something easier. The point is, you need to force strong passwords for everyone in your organization that are difficult to hack. Strong passwords should contain a combination of numbers, letters, and symbols and be at least 8 characters in length. Your IT vendor can help you automate and enforce a strong password policy throughout your network so you can rest assured your company data is protected.

   Cell phones which are used to access business data or e-mail, should require a passcode to be entered. That will go a long way toward preventing a stolen device from being compromised. Again, this can be ENFORCED by your network administrator so employees don't get lazy and choose easy-to-guess passwords, putting your organization at risk.

3. **Keep Your Network Up-To-Date.** New vulnerabilities are frequently found in common software programs you use, such as Microsoft Office and your Internet browsers; therefore, it's critical you patch and update your systems frequently. If you're under a managed IT plan, this can all be automated for you so you don't have to worry about missing an important update.

4. **Have an Excellent Backup.** This can foil the most aggressive 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, natural disasters, fire, water damage, hardware failures and a host of other data-erasing disasters. Again, your backups

should be AUTOMATED and MONITORED. Backup systems are not a set it and forget it technology. The worst time to test your backup is when you desperately need it to work!

5. **Don't Scrimp on a Good Business Grade Firewall.** A firewall acts as the frontline defense against hackers by blocking everything you haven't specifically allowed to enter (or leave) your computer network. But firewalls need monitoring and maintenance, just like all devices on your network. This too should be done by your IT vendor as part of their regular, routine maintenance.

6. **Create an Acceptable Use Policy (AUP) – And Enforce It!** 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 web sites employees can access with work devices and Internet connectivity. Further, you must enforce your policy with content-filtering software and firewalls. We can easily set up permissions and rules that will regulate what web sites specific employees access and what they do online during company hours and with company-owned devices.

7. **Implement a Mobile Device Policy.** This type of policy is particularly important if your employees are using their own personal devices to access company e-mail and data.

   If an employee is checking unregulated, personal e-mail on their own laptop which becomes infected, it can be a gateway for a hacker to enter YOUR network. What if that employee leaves, are you allowed to erase company data from their phone or mobile device? What if their phone is lost or stolen, are you permitted to remotely wipe the device – which might delete all that employee's photos, videos, texts, etc. – to ensure YOUR clients' information isn't compromised?

   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 what if that employee innocently "takes 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. These are important questions to ask when creating a Mobile Device Policy and your IT vendor should be able to help you with that too.

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 ignorant, complacent or careless, cybercriminals WILL take advantage of you. You WILL pay the ransom…NOT YOUR IT SUPPORT COMPANY that was SUPPOSED TO PROTECT YOU. This tsunami of pain will land directly on YOUR desk to deal with, and everyone will be pointing the blame at YOU, and 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 want to know for SURE that your current IT company (or IT person) is truly doing everything they can to secure your network and protect you from ransomware, bank fraud, stolen and lost data and all the other threats, problems and costs that come with a data breach, then you need to call us for a **FREE Security and Backup Audit**.

At no cost or obligation, we'll send one of our security consultants to your office to conduct our free **Security and Backup Audit** of your company's overall network health to review and validate as many as 13 different data-loss and security loopholes, including small-print weasel clauses used by many 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?

- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also help you understand how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).

- Are your employees free to use the Internet to access gambling sites, porn, and look for other jobs and waste time shopping, checking personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?

- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? 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.

- Is your firewall and antivirus configured properly and up-to-date?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." **Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in more than 150 businesses we've audited over the years.**

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

Call us now at 678-822-5815 to schedule your FREE No Obligation Security and Backup Audit!

You Are Under No Obligation to Do or Buy Anything

I also want to be very clear that there are no expectations on our part for you to do or buy anything when you take us up on our **Free Security and Backup Audit**. As a matter of fact, I will give you my personal guarantee that you won't have to deal with a pushy, arrogant salesperson because I don't appreciate heavy sales pressure any more than you do.

Whether or not we're a right fit for you remains to be seen. If we are, we'll welcome the opportunity. But if not, we're still more than happy to give you this free service.

You've spent a lifetime working hard to get where you are. You earned every penny and every client. Why risk losing it all? Get the facts and be certain your business, your reputation and your data are protected. Call us at 678-822-5815 or you can e-mail me personally at jack@zanacore.com.

Dedicated to serving you,

Jack Marder, CEO
Zanacore Technologies

Here's What Some of Our Clients Have Said:

Jim Ollick – Bus Mgr
Med-Acoustics, Inc.

"Zanacore is like having an IT expert on staff at a much reduced cost"

With today's technology, an IT person must stay up to date with all the latest changes and best practices. Zanacore has years of experience with a proven track record of doing this for us. You may find a less expensive service but, as they say, you get what you pay for, do you want your business processes relying on inexpensive questionable support or would you go with a proven support team. I know where my company puts its IT support money, and that is in Zanacore.

"We can sleep at night knowing our network servers and data are safe"

Intel recommends Zanacore support for Law Firm

Bob Penman - Sr. Partner
Graham & Penman LLP

Before Zanacore, we had experience with two other IT contractors working with our system. We went the cheap, startup route at first and we negotiated specialized deals based on fee swaps and "introduce me to your friends" pricing. While that was fantastic to start, eventually we saw service levels drop. We also had problems with inexperienced providers as they tended to miss deadlines because they weren't sufficiently staffed and they were difficult to contact when they were servicing larger customers.

"When we had server issues or key applications down, it was expensive, stressful, and unacceptable."

Then we considered the tradeoff of spending more on direct IT support cost versus the cost of downtime and our lawyers having to deal with IT issues outside our specialty. We realized that fixing something takes far longer than preventing it in the first place and you also must deal with the side effects in a failure (lost productivity, data, and hair). We knew the additional cost for better proactive support would be justified. We also had confidence Zanacore would perform based on the recommendation we received from Intel's corporate office and we have certainly been pleased with Zanacore service relative to cost. As an added bonus, we now have happier employees as well.

I found Zanacore's NetGuard pricing was very competitive when compared like for like service-wise. The pricing we received from other providers would fluctuate automatically based on the number of users or services while your NetGuard model was based more on whether changes were material. Having a fixed monthly price for our support has allowed us to budget better for IT support. We previously used to see big spikes in some months which could cause difficulty with cash flow.

"Before we switched to Zanacore we were at severe risk of catastrophic loss because numerous maintenance issues were being neglected."

We weren't getting security updates installed and our computers were subject to viruses or data breaches. The server wasn't being updated and backed up properly which was a great concern. Now I sleep better at night knowing our network is safe. I recommend Zanacore NetGuard for any business which is dependent on a reliable and stable data network.