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 PacketLogix, Inc.
Author: Terrence Boylan
16 Cutler Street, Suite 1, Warren, RI 02885
www.packetlogix.com 401-216-6425
terrence@packetlogix.com

PacketLogix Inc.

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 come flooding in.

But if your business is the victim of a cybercrime attack where the client or patient data is compromised, you will NOT get much 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 a criminal. 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:

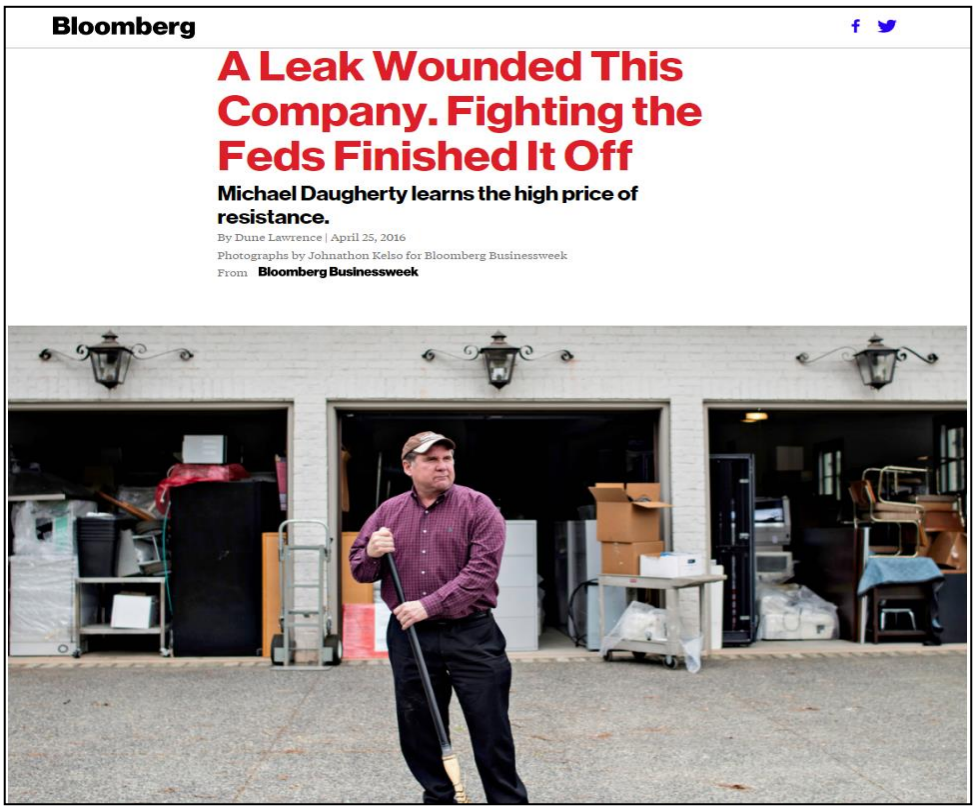
You already know that cybercrime is a very real threat to you – but it's very possible that you're underestimating the potential damage, OR **you are being ill-advised** and underserved by the employees and/or vendors you hired to protect your business from these threats.

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 on 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 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 manuals he had provided to his employees regarding cybersecurity, documentation on firewalls and penetration testing.

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

PacketLogix Inc.

"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 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 absolutely 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 actually implementing and confirming ALL of these protocols – OR if you don't know if you are – WHY NOT?

1. **The #1 Security Threat To ANY Business Is**…You! 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 on 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.

Action #1: Click this link or email paula@packetlogix.com and we will put you on our free Weekly Cybersecurity Tips list. It isn't a sales list where you get bombarded with sales emails. This is a FREE service we offer to help protect the community. We offer it to anyone, professionally or personally with no conditions or expectations on our part.

2. **Require STRONG passwords and passcodes to lock mobile devices.** Passwords should be at least 8 characters and contain lowercase and uppercase letters, symbols, and at least one number. On a cell phone, requiring a passcode to be entered 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. Are they? If you and your employees are not being forced to do a password reset every 90 days, **THEY ARE FAILING YOU**.

Action #2: Don't get overwhelmed with remembering, reusing, or recycling your passwords. Sign up for a password manager. The good ones show you how many times and where you are reused or have weak passwords, give you a score rating for all your current passwords, help you make them stronger, and even search the Dark Web for hacks involving your passwords. What's best is that they can even auto-fill in your username and password, so you don't have to remember anything!

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 updates your systems and applications when patches become available. If you're under a managed IT plan, this can all be automated for you, so you don't have to worry about an employee missing an important update.

Action #3: Directly ask your IT staff or provider to prove they are automatically patching all your computers and servers every week. If they can't provide it to you right there and then, dig into that issue. Patching is a free and easy way for you to get a lot of

protection from hackers.

4. **Have A Business-Class Image Backup BOTH On-Premises And In The Cloud.** This can foil the most aggressive (and new) ransomware attacks, where a hacker locks up your files and holds them for 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!

Action #4: Directly ask your IT staff or provider to show you the last 90 days of backup successes and failures report AND proof they are testing the full recovery of your server each week. No one cares about the backup. We care about recovery. Make sure yours works before you need it.

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 due to remote working. Thanks to the 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 smartphones for just about everything.

   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 and monitored devices, and never allow employees to access these items on personal devices or public Wi-Fi.

PacketLogix Inc.

Action #5: Ask your IT staff or provider what Mobile Device Manager (MDM) they are using, and does it have the ability to "containerize" company data on an employee's personal mobile phone separately from their photos of family, friends, and potato salad; AND can it remotely wipe that device should it get lost or stolen.

6. **A Business-Class Firewall With Monitoring.** Let's get right to the point here: a firewall your assistant buys at Staples won't cut it. Invest in a proper business-class firewall and have it installed and monitored by a seasoned professional. 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. HOWEVER, it's not uncommon for an IT guy to forget to turn on one or more of the intrusion detection and prevention features; often they are disabled to work on the firewall, but then never turned back on, making the device useless.

Action #6: Find out what firewall you are using at all your sites and is up to date with software versions and patches. Who is monitoring the alerts, and do they take action to protect you and your company?

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

Action #7: Here are three things you can do to protect your bank account.

First, separate bill paying from check signing. Most clients pay invoices online. Make sure the person paying your bills doesn't have the ability to sign checks. 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.

PacketLogix Inc.

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 the machine is automatically and continuously monitored and maintained behind your business-class firewall with up-to-date antivirus software.

Third, and lastly, contact your bank about removing the ability for wire transfers out of your account and shut down any debit cards associated with that account. If you do need debit cards, open a separate account with a very low balance. Have the debit card linked to that account. Thereby, if the debit card gets hacked, your main bank accounts aren't compromised. This is a great tactic for payroll. Only fund the payroll account after you know the exact amount needed to make that term's amount. 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. You WILL pay the ransom…NOT YOUR FAILING IT COMPANY that was SUPPOSED TO PROTECT 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 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 Business Security Score Assessment.**

PacketLogix Inc.

At no cost or obligation, we'll send one of our security consultants and a senior, certified technician to your office to conduct a **FREE Business Security Score Assessment** of your company's overall network health to review and validate different data-loss and security loopholes, including how well your physical offices are secured. 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 – and (more importantly) how FAST could you get your IT systems back online if hit with ransomware? We'll reveal exactly 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 freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check 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 they downloading illegal files (music and video) and exposing you, as happened with LabMD?

- 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 if a breach happens and the investigation reveals YOU didn't take necessary precautions – and ignorance is not an acceptable excuse that will get you out of a lawsuit.

- Is your firewall and antivirus configured properly and up-to-date? No security device is "set and forget." It needs to be constantly monitored and updated – is yours? Is your IT company giving you the assurances that it is?

- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup? Could they walk off the job with a list of all your clients and go work for a competitor?

PacketLogix Inc.

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 the hundreds of 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 third 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.

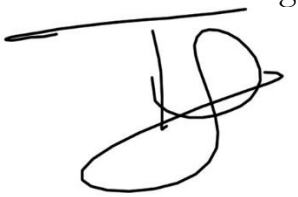
You Are Under No Obligation To Do Or Buy Anything

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 Business Security Score Assessment.** 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 this free service to you.

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 401-216-6425 or you can e-mail me personally at terrence@packetlogix.com.

Dedicated to serving you,



Terrence Boylan
CEO
PacketLogix
www.packetlogix.com
terrence@packetlogix.com

PacketLogix Inc.

Here's What A Few Of Our Clients Have Said:

Right the First Time – Every Time!

"PacketLogix brings with them an excellent understanding of all things wireless. They have the ability to design complex WLAN's, install them, and then offer day-2 support. They're a full-service shop that is able to get as deep in the weeds as necessary to implement a technology. If they don't know something, they figure it out quickly and accurately. Their size makes them extremely agile and easy to work with. Think long and hard about the personalized support you'll receive from PacketLogix, you will not find that at many of the larger firms that just aren't capable of supporting some very specialized technology. PacketLogix has always done the job right, from day 1 for as long as I've been dealing with them. How many firms can you say that about?"

Andrew K.
Network Administrator
$29 Billion Hedge Fund
New York, NY

Going Above and Beyond over a Holiday Weekend

" The single biggest benefit to our company—and to me personally—has been the speed and accuracy with which your solution got us back up and running. That I could call the last business day before a holiday weekend and have you here within the hour to pick up our hard drive, hear by early evening that your attempted recovery was a success, have someone work through the night to extract all the data, and then have you deliver a full solution back to us in days—even with the Christmas holiday—sets you in a league of your own. Your approach and professionalism was second to none."

Ellen McNulty-Brown
Chief Executive Officer
Lotuff Leather
Providence, RI

"Often professional service companies claim to provide a host of services and succeed on some but fail on others. PacketLogix succeeded across the board and truly provided a full-service solution that exceeded expectations at every turn and function."

"People should pick their professional service partners based on honesty and integrity—especially when data is a consideration. Terrence and his team were truly engaged and partnered to address all the challenges that presented to our business. Their concern was that we would experience as little downtime as possible and that we would be receiving exactly what we needed in as efficient a manner as possible. I trust Terrence, and I appreciate everything that his team provided to restore our data and reporting."

PacketLogix Inc.

Dedicated to Customer Success.

"One major benefit of working with PacketLogix is the recent transition to a more stable and robust Wi-Fi system. It is comforting to understand you know the product you sold me inside and out. The installation and deployment went smoothly. The bottom line for us is that Terrence and his team are dedicated to customer success, and they're nice people."

Brett Smith, Partner
FUSE Sports Marketing
Burlington, Vermont

Security Delivered!

"We are a full-service boatyard and require a completely secure technology environment that protects our business. PacketLogix continues to be our go-to for our network IT, security, and security cameras. The team has very sharp engineers and excellent customer service. Their pricing is also competitive while delivering high value. I am extremely happy with their service and solutions and recommend that you give them an opportunity to serve you as well."

Brad Niemiec, President
Niemiec Marine
New Bedford, MA

A Dream Come True!

"As the owner of a small business, my time is at a premium. PacketLogix takes all IT and technology decisions off my plate so I can focus on other aspects of my business where I am needed. Terrence and his team are personable and knowledgeable and are a great resource for a business of any size."

"They are the only IT firm I will work with. Call and talk to Terrence now!"

Maria Martinez, Co-Founder
Whetstone Workshop
Providence, RI

PacketLogix Inc.

A Valued Extension Of Our Team

Cynthia Fanikos
Chief Financial Officer
St. Johns Prep
Danvers, MA

“While working with PacketLogix we’ve had several positive experiences. The first was the successful full integration of a new wireless system that was completed in a very short period, and the successes have only continued from there. PacketLogix works with our school in a partnership format. They listen to our IS team to better understand the issues and then come back with potential solutions that integrate within our existing systems and culture. They are always readily available for questions in regard to current projects, best practices, and industry standards.”

“To someone on the fence, I would tell them that the team at PacketLogix uses an approach by which they become an extension of the IS team. By doing this, there is a natural integration and transfer of knowledge from PacketLogix to the internal team as well as a respect and understanding of the underlying school's e