

THE CYBER SECURITY CRISIS

URGENT AND CRITICAL PROTECTIONS WE ARE URGING ALL
CLIENTS TO HAVE IN PLACE NOW TO PROTECT THEIR BANK ACCOUNTS,
CLIENT DATA, CONFIDENTIAL INFORMATION AND REPUTATION FROM
THE TSUNAMI OF CYBERCRIME

The growth and sophistication of cybercriminals, ransomware and hacker attacks has reached epic levels, and NEW protections are now required. We have created this report to inform our private clients about what's going on and educate them on new protections we are urging you to put in place.



Notice: This publication is intended to provide accurate and authoritative information regarding the subject matter covered. However, no warranties are made. It is provided with the understanding that the author and the publisher are NOT engaged in rendering legal, accounting or related professional services or advice and that this publication contains opinions of its author. This publication is NOT intended as a substitute for specific legal or accounting advice for any particular institution or individual. The publisher accepts NO responsibility or liability for any individual's decisions or actions made as a result of information or opinion contained herein.

Provided by:

Hodgson Consulting & Solutions, Ltd

Author: Robert Zehnder

1110 W. Lake Cook Road, Suite 235

www.hodgsonconsulting.com

847-906-5005

IF YOU FALL VICTIM TO A CYBER-ATTACK BY NO FAULT OF YOUR OWN, WILL THEY CALL YOU CARELESS...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 support comes flooding in, as it should.

But if your business is the victim of a cybercrime attack where YOUR client or patient data is compromised, you will NOT get such sympathy. You will be labeled careless and irresponsible. **You may even 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 have protections in place. Claiming ignorance is not an acceptable defense, and this giant, expensive and potentially reputation-destroying nightmare will land squarely on YOUR shoulders.



But it doesn't end there...

According to the laws here in IL, you will be required to notify your clients when there is a breach or notice of breach. The notification must be made “without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the data system.”

If it becomes public, your competition will have a heyday over this. Clients will be IRATE and will take their business elsewhere. Morale will tank and employees may even 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.



 www.hodgsonconsulting.com
 1110 W. Lake Cook Road, Suite 235,
Buffalo Grove, IL

WHY WE WROTE THIS REPORT FOR OUR CLIENTS

Over the last year, there has been a significant increase in the sophistication, frequency and severity of cybercrime attacks.

We've been watching these trends and putting in place new technologies, protocols and services to protect our clients. Some we've been able to include in our normal fees and services to you – but some are newer, more effective and would be an add-on or replacement for what you have now, which requires us to take a closer look at your current protections and make recommendations based on your specific situation.

To prepare you for our discussion, we've compiled this report to educate you and provide details on why we are making these recommendations.



YES, IT CAN HAPPEN TO YOU AND THE DAMAGES ARE VERY REAL

The biggest challenge we face in protecting YOU and our other clients is that many stubbornly believe

“That won’t happen to me” because they’re “too small” or “don’t have anything a cybercriminal would want.” Or they simply think that if it happens, the damages won’t be that significant. That may have held true 10 to 20 years ago, BUT NOT TODAY.

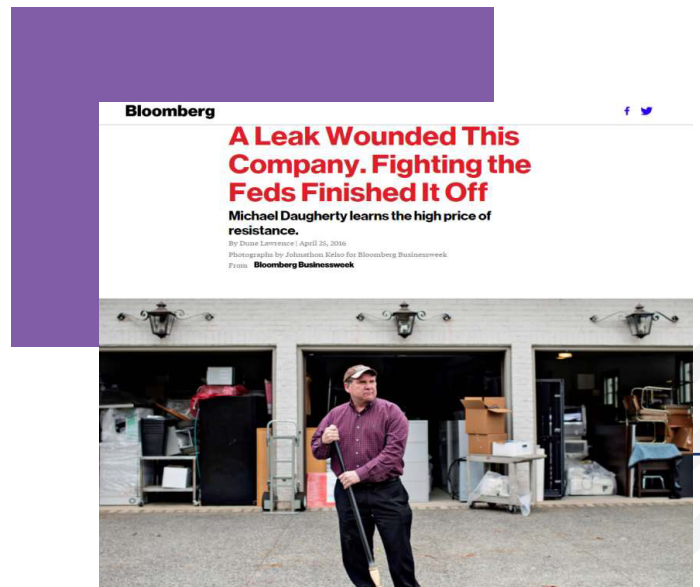
Consider the story of Michael Daugherty, former CEO of LabMD. His small, Atlanta-based company tested blood, urine and tissue samples for urologists – a business that was required to comply with federal rules on data privacy as outlined in the Health Insurance Portability and Accountability Act, or HIPAA.

He HAD an internal 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. A simple, innocent mistake made by a tenured, honest employee that was not caught by the IT department.

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 shared on the situation was “inadequate”; in-person testimony by the staff regarding the breach was requested, as well as more details on what training manuals he had provided to his employees regarding cyber security, documentation on firewalls and penetration testing. (IMPORTANT: This is a new service we are now making available to our clients for this very reason.)



Long story short, his employees blamed HIM and left, looking for more “secure” jobs at companies that weren’t under investigation. Sales steeply declined as clients took their business elsewhere. His insurance providers refused to renew their policies.

The FTC relentlessly pursued him with demands for documentation, testimonies and other information he had already provided, sucking up countless hours of time. 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, storing what was left of the medical equipment he owned in his garage, where it remains today.

“NOT MY COMPANY...NOT MY PEOPLE...WE’RE TOO SMALL” YOU SAY?

Don’t think you’re in danger because you’re “small” and not a big company like Experian, J.P. Morgan or Target? That you have “good” people and protections in place? That it won’t happen to you?

That’s EXACTLY what cybercriminals are counting on you to believe. It makes you easy prey because you put ZERO protections in place, or grossly inadequate ones.



Look: Over 82,000 NEW malware threats are being released every single day, and HALF of the cyberattacks occurring are aimed at small businesses; you just don’t hear about it because the news wants to report on BIG breaches OR it’s kept quiet by the company for fear of attracting bad PR, lawsuits and databreach fines, and out of sheer embarrassment. But make no mistake – small, “average” businesses are being compromised daily, and clinging to 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 includes only the ones that were reported. Most small businesses are too embarrassed or afraid to report breaches, so it’s safe to assume that the number is much, much higher.

Are you “too small” to be significantly damaged by a ransomware attack that locks all of your files for several days or more?

Are you “too small” to deal with a hacker using your company’s server as “ground zero” to infect all of your clients, vendors, employees and contacts with malware? Are you “too small” to worry about someone taking your payroll out of your bank account? According to Osterman Research, the AVERAGE small business lost over \$100,000 per ransomware incident and over 25 hours of downtime. Of course, \$100,000 isn’t the end of the world, is it? But are you okay to shrug this off? To take the chance?



 www.hodgsonconsulting.com
 1110 W. Lake Cook Road, Suite 235,
Buffalo Grove, IL

IT'S NOT JUST CYBERCRIMINALS WHO ARE THE PROBLEM

Most business owners erroneously think cybercrime is limited to hackers based in China or Russia, but the evidence is overwhelming that disgruntled employees, both of your company and your vendors, can cause significant losses due to their knowledge of your organization and access to your data and systems. What damage can they do?

- **They leave with YOUR company's files, client data and confidential information stored on personal devices**, as well as retaining access to cloud applications, such as social media sites and file-sharing sites (Dropbox or OneDrive, for example) that you aren't even aware they were using. In fact, according to an in-depth study conducted by Osterman Research, **69% of businesses experience data loss due to employee turnover and 87% of employees who leave take data with them.** What do they do with that information? Sell it to competitors, BECOME a competitor or retain it to use at their next job.
- **Funds, inventory, trade secrets, client lists and HOURS stolen.** There are dozens of sneaky ways employees steal, and it's happening a LOT more than businesses care to admit. According to the website StatisticBrain, 75% of all employees have stolen from their employers at some point. From stealing inventory to check and credit card fraud, your hard-earned money can easily be stolen over time in small amounts that you never catch.

But here's the most COMMON way they steal: They waste HOURS of time on your dime to do personal errands, shop, play games, check social media feeds, gamble, read the news and a LONG list of non-work-related activities. Of course, YOU are paying them for a 40-hour week, but you might only be getting some of that. Then they complain about being "overwhelmed" and "overworked." They tell you, "You need to hire more people!" so you do. All of this is a giant suck on profits if you allow it. Further, if we don't put in place web security filtering to limit what sites they can visit (and we certainly do have this for many clients), they could do things that put you in legal jeopardy, like downloading illegal music and video files, visiting adult-content websites, gaming and gambling – all of these sites fall under HIGH RISK for viruses and phishing scams. (IMPORTANT: We now have solutions to prevent this that we are rolling out to clients who want to stop this from happening to them.)

- **They DELETE everything. A common scenario:** An employee is fired or quits because they are unhappy with how they are being treated – but before they leave, they permanently delete ALL their e-mails and any critical files they can get their hands on. If you don't have that data backed up, you lose it ALL. Even if you sue them and win, the legal costs, time wasted on the lawsuit and on recovering the data, not to mention the aggravation and distraction of dealing with it all, involve a far greater cost than what you might get awarded, might collect in damages. (IMPORTANT: For all Signature Service Clients, we are confident we could get the data back; but for clients who are not under that plan, or who do not have our SafetyNet backup solution, you are vulnerable to this.)

Do you *really* think you are immune to any or all of this happening to you?

Then there's the threat of vendor theft. Your payroll, HR and accounting firm have direct access to highly confidential information and a unique ability to commit fraud. THEIR employees, not just the leadership team, can steal money, data and confidential information. All it takes is a part-time employee – perhaps hired to assist in data entry during tax season, and who is not being closely supervised or is working from home on routine tasks with your account – to decide to make a little money on the side by selling data or siphoning funds from your account.

EXACTLY HOW CAN YOUR COMPANY BE DAMAGED BY CYBERCRIME? LET US COUNT THE WAYS:

IMPORTANT: Clients who are on our Signature Service plan DO have protections in place to greatly reduce the chances of these things happening, and the severity and impact if they get compromised. You should also know there is absolutely no way we, or anyone else, can 100% guarantee you won't get compromised – you can only put smart protections in place to greatly reduce the chances of this happening, to protect data so it IS recoverable and to demonstrate to your employees, clients and the lawyers that you WERE responsible and not careless.

You should also know we are actively reviewing ALL clients' networks and specific situations to recommend NEW protections we feel you should have in place.



1. **Reputational Damages:** What's worse than a data breach? Trying to cover it up. Companies like Yahoo! are learning that lesson the hard way, facing multiple class-action lawsuits for NOT telling their users immediately when they discovered they were hacked. With Dark Web monitoring and forensics tools, WHERE data gets breached is easily traced back to the company and website, so you cannot hide it.

When it happens, do you think your clients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers: HAVE YOU BEEN RESPONSIBLE in putting in place the protections outlined in this report, or will you have to tell your clients, "Sorry, we got hacked because we didn't think it would happen to us" or "We didn't want to spend the money." That will not be sufficient to pacify them.

2. **Government Fines, Legal Fees, Lawsuits:** Breach-notification statutes remain one of the most active areas of the law. Right now, several senators are lobbying for "massive and mandatory" fines and more aggressive legislation pertaining to data breaches and data privacy. The courts are NOT in your favor if you expose client data to cybercriminals.

Don't think for a minute that this applies only to big corporations: ANY small business that collects customer information also has important obligations to its customers to tell them if they experience a breach. In fact, 47 states and the District of Columbia each have their own data breach laws – and they are getting tougher by the minute. If you're in health care or financial services, you have



 www.hodgsonconsulting.com
 1110 W. Lake Cook Road, Suite 235,
Buffalo Grove, IL


additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). Among other things, HIPAA stipulates that if a health care business experiences a breach involving more than 500 customers, **it must notify a prominent media outlet about the incident.** SEC and FINRA also require financial services businesses to contact them about breaches, as well as any state regulatory bodies.

One of the things we want to discuss with you is how to ensure you are compliant and you stay compliant.

- 3. Cost, After Cost, After Cost:** ONE breach, one ransomware attack, one rogue employee you are not protected against, can create HOURS of extra work for staff who are already maxed out when things are going well. Then there's business interruption and downtime, backlogged work delivery for your current clients. Loss of sales. Forensics costs to determine what kind of hack attack occurred, what part of the network is/was affected and what data was compromised. Emergency IT restoration costs for getting you back up, if that's even possible. In some cases, you'll be forced to pay the ransom and maybe – just maybe – they'll give you your data back. Then there are legal fees and the cost of legal counsel to help you respond to your clients and the media. Cash flow will be significantly disrupted, budgets blown up. Some states require companies to provide one year of credit-monitoring services to consumers affected by a data breach and more are following suit.

According to the Cost of Data Breach Study conducted by Ponemon Institute, **the average cost of a data breach is \$225 per record compromised, after factoring in IT recovery costs, lost revenue, downtime, fines, legal fees, etc.** How many client records do you have? Employees? Multiply that by \$225 and you'll start to get a sense of the costs to your organization. [NOTE: Health care data breach costs are the highest among all sectors.]

- 4. Bank Fraud:** If your bank account is accessed and funds stolen, the bank is NOT responsible for replacing those funds. Take the true story of Verne Harnish, CEO of Gazelles, Inc., a very successful and well-known consulting firm, and author of the best-selling book *The Rockefeller Habits*. Harnish had \$400,000 taken from his bank account when hackers were able to access his PC and intercept e-mails between him and his assistant. The hackers, who are believed to be based in China, sent an e-mail to his assistant asking her to wire funds to 3 different locations. It didn't seem strange to the assistant because Harnish was then involved with funding several real estate and investment ventures. The assistant



responded in the affirmative, and the hackers, posing as Harnish, assured her that it was to be done. The hackers also deleted his daily bank alerts, which he didn't notice because he was busy running the company, traveling and meeting with clients. That money was never recovered and the bank is not responsible. Everyone wants to believe "Not MY assistant, not MY employees, not MY company" – but do you honestly believe your staff is incapable of making a single mistake? A poor judgment? **Nobody believes they will be in a car wreck when they leave the house every day, but you still put the seat belt on.** You don't expect a life-threatening crash, but that's not a reason to not buckle up. *What if?*

- 5. Using YOU As The Means To Infect Your Clients:** Some hackers don't lock your data for ransom or steal money. Often they use your server, website or profile to spread viruses and/or compromise other PCs. If they hack your website, they can use it to relay spam, run malware, build SEO pages or promote their religious or political ideals. (Side note: This is why you also need advanced endpoint security, spam filtering, web gateway security, SIEM and the other items detailed in this report, but more on those in a minute.)

[To be clear, clients under our Security Plus plan would greatly reduce their risk against THIS happening.]

HERE IS OUR CURRENT LIST OF PROTECTIONS YOU SHOULD HAVE IN PLACE NOW

Below is a list of things we recommend all clients have in place ASAP. **Some you may already have, and some may be lacking, which is why we are currently contacting all clients to conduct a review of their current situation.**

We are also working to implement better tools, protocols and documentation, and will be sharing these updates with you as they come available, and in our Quarterly Technology Reviews for clients on our Signature Service plan.

☐ **QBRs Or Quarterly Business Reviews And Security Risk Assessments:** We will be more persistent in scheduling and holding these meetings with ALL clients. During these consultations, we will conduct a security risk assessment and provide you with a score. We will also brief you on current projects, review your IT plan and budgets, discuss NEW tools and solutions we feel you may need, and make recommendations. We will also answer any questions you have and make sure you are satisfied with our services.

☐ **Proactive Monitoring, Patching, Security Updates:** This is what we deliver in our Peace of Mind Business Solutions Signature Managed IT Services Plan. Specifically, we provide:

- 24/7 Network Monitoring
- Monthly Executive Summary Reporting
- Client Access to Help Center Online Portal
- Virus Definition and Security Patch Updates
- Spyware Monitoring and Removal
- Help Desk Support
- Install Software Upgrades
- Microsoft Office Professional Plus Licenses
- Monthly Network Tune Ups
- Quarterly On-Site Consultation
- A Year End Technology Review

- ☐ **[NEW!] Insurance Review:** At least once a year, we will perform a Cyber Insurance Audit for YOU. We can also work with your insurance agent to review your cyber liability, crime and other relevant policies to ensure we, as your IT company, and you, as a company, are fulfilling their requirements for coverage
- ☐ **[NEW!] Data Breach And Cyber-Attack Response Plan:** This is a time-and-cost-saving tool as well as a stress-reduction plan. We will be working with our clients to create and maintain a cyberresponse plan so that IF a breach happens, we could minimize the damages, downtime and losses, and properly respond to avoid missteps.
- ☐ **Ransomware Backup And Disaster Recovery Plan:** One of the reasons the WannaCry virus was so devastating was because it was designed to find, corrupt and lock BACKUP files as well. That's why we are insisting clients upgrade to our SafetyNet backup solution, which is included in our Signature Managed IT Services Plan.
- ☐ **[NEW!] A Mobile And Remote Device Security Policy:** All remote devices – from laptops to cell phones – need to be backed up, encrypted and have a remote “kill” switch that would wipe the data from a lost or stolen device. You also need to have a policy in place for what employees can and cannot do with company-owned devices, how they are to responsibly use them and what to do if the device is lost or stolen.
- ☐ **More Aggressive Password Protocols:** Employees choosing weak passwords are STILL one of the biggest threats to organizations. To protect against this, we will require a monthly password update for all employees and put in place controls to ensure weak, easy-to-crack passwords are never used. We will also have checklists for employees who are fired or quit to shut down their access to critical company data and operations.
- ☐ **[NEW!] Advanced Endpoint Security:** There has been considerable talk in the IT industry that antivirus is dead, unable to prevent the sophisticated attacks we're seeing today. That's why we are recommending all clients UPGRADE to our Security Plus Plan.

- ☐ **Multi-Factor Authentication:** Depending on your situation, we will be recommending multifactor authentication for access to critical data and applications.
- ☐ **Web-Filtering Protection:** Porn and adult content is the #1 thing searched for online, most often during the 9-to-5 workday. Online gaming, gambling and file-sharing sites for movies and music are also ranked in the top searches and are “click bait” hunting grounds for hackers. These are sites you do NOT want your employees visiting during work hours on company-owned devices. If your employees are going to infected websites, or websites you DON'T want them accessing at work, they can not only expose you to viruses and hackers, but they can also get you nailed for sexual harassment and child pornography lawsuits – not to mention the distraction and time wasted on YOUR payroll, with YOUR company-owned equipment. All of this can (and should) be blocked from company-owned Internet and devices.
- ☐ **[NEW!] Cyber Security Awareness Training:** Employees accidentally clicking on a phishing email or downloading an infected file or malicious application is still the #1 way cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously. We have several new solutions we can discuss with you to inform and remind your employees to be on high alert and reduce their likelihood of clicking on the wrong email or succumbing to other scams.
- ☐ **Protections For Sending Confidential Information Via E-mail:** Employees have access to a wide variety of electronic information that is both confidential and important. That's why we'll be ensuring all clients' e-mail systems are properly configured to prevent the sending of protected data.
- ☐ **Secure Remote Access Protocols:** You and your employees should never connect remotely to your server or work PC using GoToMyPC, LogMeIn or TeamViewer. Remote access should strictly be via a secure VPN (virtual private network). For our clients who need this type of access, we will be implementing proper technologies that are secure.
- ☐ **[NEW!] Dark Web/Deep Web ID Monitoring:** There are new tools available that monitor cybercrime websites and data for YOUR specific credentials being sold or traded. Once such breaches are detected, these tools notify you immediately so you can change your password and be on high alert.

OUR PREEMPTIVE CYBER SECURITY RISK ASSESSMENT WILL GIVE YOU THE ANSWERS YOU WANT, THE CERTAINTY YOU NEED

On our own initiative, we have conducted a more thorough, CONFIDENTIAL investigation of your computer network, backups and security protocols as outlined in this report and have generated a custom “Risk Assessment Health Score.”

This score is based on a number of factors including, but not limited to, the type of data you have, regulatory compliance you may need to adhere to and other unique factors such as the number of employees you have, locations, nature of your business, etc.

We have also conducted a recent Dark Web scan of your and your employees’ credentials and will share those results with you during our meeting. This scan will reveal if your or any of your employees’ usernames and passwords are being sold to cybercriminals via the Dark Web.

We will be sharing those results, along with your Risk Assessment Health Score, during the meeting we’ve booked.



PLEASE...DO NOT JUST SHRUG THIS OFF

(HOW TO PREPARE FOR OUR CONSULTATION)

To get the most out of our upcoming meeting, I would suggest you share this report with your executive team and invite them to our consultation (if appropriate).

If you have any questions, **call us at 847-906-5005 or send me an e-mail to rzehnder@hodgsonconsulting.com.**

I know you are extremely busy and there is enormous temptation to discard the warnings around cyber security, 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 have to deal with a cyber security "event," be it an employee issue, serious virus or ransomware attack.

The purpose of our meeting to make sure you are brilliantly prepared for it and experience only a minor inconvenience at most. But if you wait and do nothing and ignore our advice, I can practically guarantee this will be a far more costly, disruptive and devastating disaster.

You've spent a lifetime working hard to get where you are today. Let us help you protect and preserve it. Give you complete peace of mind.

Dedicated to serving you,



Robert Zehnder

Web: www.hodgsonconsulting.com

E-mail: rzehnder@hodgsonconsulting.com

Direct: 847-906-5005



 www.hodgsonconsulting.com
 1110 W. Lake Cook Road, Suite 235,
Buffalo Grove, IL