ESSENTIAL IT SERVICES, INC
IT Promises: Delivered!

The Cyber Security Crisis

Managing The Cyber Crisis

Urgent And Critical Protections Every CEO and Business Owner Must 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. CEOs can no longer ignore it or foolishly think "that won't happen to us."

Your business – large OR small – will be targeted and will be compromised UNLESS you take action on the information revealed in this shocking new executive report.

When You Fall Victim To A Cyber-Attack By 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 support comes flooding in, as it should.

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

According to Kansas laws, you will be required to tell your clients and/or patients that YOU exposed them to cybercriminals. Your competition will have a heyday over this. Clients will be IRATE and leave in droves. Morale will TANK and employees will BLAME YOU. Your bank is NOT required to replace funds stolen due to cybercrime (go ask them), and unless you have a very specific type of insurance policy, any financial losses will be denied coverage.

Please do NOT underestimate the importance and likelihood of these threats. It is NOT safe to assume your IT team (or company) is doing everything they should be doing to protect you; in fact, they are NOT, which we can demonstrate with your permission.

Yes, It CAN Happen To YOU And The Damages Are VERY Real

You might already know about the escalating threats, from ransomware to hackers; but it's very possible you are the risk to your company. If you believe that cybersecurity is an "IT problem" and that it can be solved by "better tools" then you are at serious risk of experiencing the worst outcomes from a cybersecurity incident when, not if, it occurs.

This is not a topic to be casual about. Should an incident occur, your reputation, your money, your company and your neck will be on the line, which is why you must get involved and make sure your company is prepared and adequately protected, not just pass this off to someone else.

This Is Too Serious A Matter To Entrust To Others And Completely Delegate Without Your Involvement

This is no longer an issue that can simply be delegated to the IT department.

ONE slipup from even a smart, tenured employee clicking on the wrong e-mail, innocently downloading an application, lazily using an easy-to-remember password for ONE application, is all it takes to open the door to a hacker or ransomware and **create real damage**.

Take 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 must have believed that his IT team had put in place tools that would protect them from a data breach – or maybe he mistakenly thought that being compliant was the same as being 'safe' from a cyber attack. Unfortunately, neither of those concepts were true, as the manager of his billing department was still 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 bad actor 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 bad actor 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. **(QUESTION: ARE YOU DOING ANY OF THIS NOW?)**

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 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 into his garage, where it remains today.

“Being Compliant Is Not Being Safe, and Being Safe Is Not Being Compliant”

Many CEOs and Business Owners mistakenly believe that cybersecurity is an IT function. In reality, they are two distinctly different business roles with distinctly different goals. The function of IT is to keep your technology running, maximizing productivity and efficiency, and maximizing return on investment in your IT infrastructure. The function of Cybersecurity is to assess the business risk associated with cyber security attacks and to assist CEOs and Business owners in devising strategies to either accept, mitigate, or transfer that risk.

“Not My Company…Not My People… We’re Too Small” You Say?

Don’t think you’re not 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: 82,000 NEW malware threats are being released every single day, and HALF of the cyber-attacks 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 data-breach 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 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?

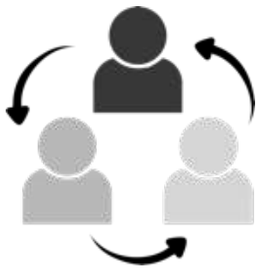
It's NOT Just Cybercriminals Who Are The Problem

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).

  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.



- **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. 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.

- **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 is a far greater cost than what you *might* get awarded, might collect in damages.

Do you *really* think this *can't* happen 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:

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/patients 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." Is *that* going to 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 only applies to big corporations: ANY 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 additional notification requirements under the Health Insurance Portability and Accountability Act (HIPAA), theFederal Trade Commission (FTC) Safeguards Rule, and the Payment Card Industry (PCI) Data Security Standard (DSS). Among other things, HIPAA and the FTC Safeguards rule both stipulates that if a business experiences a breach involving more than 500 customers, it must notify a prominent media outlet about the incident. The FTC also requires financial services businesses to contact them about breaches.

With all the new laws being passed, there is a very good chance you are NOT compliant.

3. Cost, After Cost, After Cost:

ONE breach, one ransomware attack, one rogue employee 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 that 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?

Claiming ignorance is not a viable defense, nor is pointing to your outsourced IT company to blame them. YOU will be responsible, and YOUR company will bear the brunt.

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.

You May Want To Believe You're "Safe" But A Preemptive Independent Risk Assessment Is: The **ONLY** Way You Can Really Be Sure

While there is no way to entirely prevent cyber attack short of taking your entire business offline (which is unreasonable for a business transacting today), there ARE things you can do to dramatically reduce the chances of getting attacked and minimize the loss and negative impact it will have. If you want to be BRILLIANTLY prepared instead of caught completely off guard, here are 5 things you MUST do now.

It will start with a Security Assessment. A Security Assessment is exactly what it sounds like – it's a process to review, evaluate and "stress test" your company's network to uncover loopholes and vulnerabilities BEFORE a cyber-event happens.

Just like a cancer screening, a good assessment can catch problems while they're small, which means they will be a LOT less expensive to fix, less disruptive to your organization AND give you a better chance of surviving a cyber-attack.

An assessment should always be done by a qualified 3rd party, NOT your current IT team or company; fresh eyes see things hidden, even in plain sight, from those looking at it daily.

You want a qualified "Sherlock Holmes" investing on YOUR behalf who is not trying to cover up inadequacies or make excuses, bringing to you a confidential report you can use before others find dirty laundry and air it in harmful ways.

Our Free Cyber Security Risk Assessment Will Give You The Answers You Want, The Certainty You Need

For a limited time, we are offering to give away a Free 5-Step Ransomware Prevention Consultation to a select group of businesses. This is entirely free and without obligation. EVERYTHING WE FIND AND DISCUSS WILL BE STRICTLY CONFIDENTIAL.

This assessment will provide verification from a **qualified third party** on whether or not your current IT team, or company, is doing everything they should to keep your computer network not only up and running, but as safe as possible from cybercrime.

Here's How It Works: At no cost or obligation, schedule a 30-minute telephone consultation to start the process. During the phone call, we will launch a non-invasive, CONFIDENTIAL investigation of your computer network, backups, and security protocols. Your current IT team, or company, DOES NOT NEED TO KNOW we are conducting this assessment. We will not install any software on your devices, and you won't need to know any passwords. Your time investment is minimal: 30 minutes for the initial meeting and one hour in the second meeting to go over our Report Of Findings.

When this Risk Assessment IS complete, you will know:

- **If you and your employees' login credentials are being sold on the Dark Web.** We will run an initial scan on one computer during the initial phone call and follow up with more scans after the meeting concludes. The results will NOT be e-mailed or otherwise shared with anyone but you, in person, at the second meeting). It's RARE that we don't find compromised credentials – and I can guarantee what we find will shock and alarm you.

- IF your I.T. systems and data are **truly secured** from hackers, cybercriminals, viruses, worms and even sabotage by rogue employees.

- IF your **current backup would allow you to be back up and running again fast** if ransomware locked all your files. *In 99% of the computer networks we've reviewed over the years, the owners were shocked to learn the backup they had would NOT survive a ransomware attack.*

- IF you have Personally Identifiable Information on your network, we can detect it quickly and stop the cyber criminals before they do extensive damage.

If we DO find problem–overlooked security loopholes, inadequate backups, credentials that have been compromised, out-of-date firewall and antivirus software and (often) active malware—on one or more of the PCs in your office, we will propose an Action Plan to remediate the situation that you can have us implement for you if you choose.

Visit **www.essentialits.com** or call our office at **316.867.4566**

Again, I want to stress that EVERYTHING WE DISCUSS AND DISCOVER WILL BE <u>STRICTLY CONFIDENTIAL</u>.

Why Free?

Frankly, we want the opportunity to assist you in your cybersecurity journey. We know we are the most competent, responsive, and trusted cybersecurity and IT services providers to small businesses in South Central Kansas.

However, I also realize **there's a good chance you've been burned, disappointed and frustrated by the complete lack of service and the questionable advice** you've gotten from other IT companies in the past. In fact, you might even be so overwhelmed by the news of big corporations and even the United States government getting hacked, that you just want to give up and ignore cybersecurity altogether. *I don't blame you.*

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

Please...Do NOT Just Shrug This Off *(What To Do Now)*

I know you are *extremely busy* and there is enormous temptation to discard this, shrug it off, worry about it "later" or dismiss it altogether. That is, undoubtedly, the easy choice... but the easy choice is rarely the RIGHT choice. **<u>This I can guarantee:</u>** At some point, you WILL HAVE TO DEAL WITH A CYBER SECURITY EVENT.

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

You've spent a lifetime working hard to get where you are today. Don't let some lowlife thief operating outside the law in another country get away with taking that from you. And certainly don't "hope" your IT team, or company, has you covered, no matter how expensive the tools you buy them.

Get the facts and be certain you are protected.

Contact us and schedule your Free, CONFIDENTIAL Cyber Security Risk Assessment today: www.essentialits.com/security. Feel free to also reach out to me direct at the phone number and e-mail address below.

Contact Us And Schedule Your Free, CONFIDENTIAL Cyber Security Risk Assessment Today!

Dedicated to serving you,

JD Zluticky
Web: www.essentialits.com
E-mail: jdzluticky@essentialits.com
T: 316.867.4566

P.S. – When I talk to other cybersecurity professionals like myself, and CEOs / Business Owners who have been hacked or compromised, almost all of them told me they thought their IT team, or company, "had things covered." Again, your IT team, or company, cannot have you covered because they are not focused on the business risk of a cybersecurity attack. This is why you need a preemptive, independent risk assessment like the one I'm offering in this letter.

As a CEO myself, I understand that you have to delegate and trust, at some level, that your employees and vendors are doing the right thing – but it never hurts to validate that they are. Remember, it's YOUR reputation, YOUR money, YOUR business that's on the line. THEIR mistake is YOUR nightmare.


ESSENTIAL IT SERVICES, INC
IT Promises: Delivered!


ESSENTIAL IT SERVICES, INC
IT Promises: Delivered!