CYBER SECURITY GUIDE

FOR SMALL BUSINESSES

www.troinet.com

troinet

engage@troinet.com

THE HARSH JUDGMENT

In the event that you fall victim to a cyber-attack without proper cybersecurity, you are at risk of being judged as "careless and incompetent."

Yes, this is harsh. But the moment hackers breach your system and access any type of employee, patient, or customer data, you will get NO COMPASSION. You will immediately be labeled stupid and incompetent.

Investigations

Both government authorities and clients might investigate your business why this breach happened under your watch.

Trust and respect may diminish, and employees may even fault you. Your bank is not required to replace funds stolen due to cybercrime (go ask them)

If they find out that you did not implement the security measures that we outlined in this guide, you can be held liable and be slapped with serious fines and lawsuits. Claiming ignorance of the law is obviously not a defense. As a business owner, you will not carry the heavy burden of answering complaints that carry with them costly, goliath, and reputation-destroying nightmares.

Yet, it does not end there…

Loss of Income

As per the laws of most states, you will be obliged to inform your clients and even the public that you have exposed their data to cyber criminals so that proper responses can be made. If that happens, your competitors will go on celebration mode over it. Your Customers will get furious and will find other providers.

Trust and respect may diminish, and employees may even fault you. Your bank is not required to replace funds stolen due to cybercrime (go ask them), and any monetary misfortunes will be denied by insurance companies unless you have a very special kind of insurance policy for cybercrime.

We beg you not to take these risks and threats too lightly.

WHY WE WROTE THIS REPORT FOR OUR CLIENTS AND AUDIENCE

In the last few months, hackers have become more advanced, aggressive, and ruthless. The damage produced by such attacks are ballooning through time, and as a response, Congress have been legislating new guidelines requiring businesses to step-up information security and protection or face solid sanctions.

To aggravate the situation, COVID-19 forced organizations to quickly send their employees to work remotely without a solid security protocol. This compromised many business and exposed vulnerable data to less secured conditions. The pandemic situation has likewise awakened the excitement of cyber criminals who are eager to increase their exploits during this global crisis.

In fact, the FBI announced that cyber-attacks grew 4x during the pandemic.

We have been monitoring these patterns and setting up solutions such as secured network services, network security services, IT support to ensure the safety of our customers. We innovate in not just

offering a piece of software or hardware, but we embed our own skill in IT security with every piece of service we offer.

Some of these we offer as a stand-alone service, and some are add-ons to existing services that our clients have now. On a regular basis, we assess our clients' present security situation and make tailored suggestions based on their circumstance.

To assist your understanding, we have created this report to help you understand why we are doing what we do.

Caution: This Cyberattack CAN Happen To YOU And the Damages May be Beyond You Can Bear

Our greatest challenge in protecting YOU and other customers is resistance. Many business owners keep on saying to themselves, "this won't happen to me" or "I have nothing that hackers want." Or subconsciously they think that in case the hacking occurs, the harm will not be that huge. Ten or twenty years ago that could be true, but NOT TODAY.

A MAN WHO SPENT YEARS IN CYBERSECURITY LEGAL BATTLES BECAUSE OF "ONE SMALL IT SECURITY MISTAKE"

Here's the true story of Michael Daugherty, former CEO of LabMD.

He had a medical testing lab in Atlanta where they conducted blood tests, urine tests, and tissue samples for urologists. His business obliged to comply with government rules such as HIPAA Regulations (Health Insurance Portability and Accountability Act) which revolves around data privacy.

He hired an internal IT group with the belief that they can protect the business from cyber hackers - yet the billing department manager wanted to listen to music and downloaded a peer-to-peer file-sharing software. However, she accidentally left her documents folder open (which contained more than 9,000 patient documents) and that was used as entry point by other users of that file-sharing network. It was accessed and taken without permission.

Sounds like a "small and harmless" mistake by a tenured employee! Michael Daugherty back then also thought that these are being taken care of by his IT team.

The billing manager's mistake enabled IT-skilled individuals to hack in, access the document and use it against LabMD for blackmail. At the point when Daugherty refused to pay them a "ransom", the organization detailed a report to the Federal Trade Commission, who at that point came thumping on Michael's doors.

The employees left and searched for another employer not under government scrutiny and can give them better job security. Daugherty lost large amounts of clients as many of them switched to other providers.

After spending sleepless nights, stressful days, and approximately 5000 pages of pleadings to Washington, the Court simply responded that his filing was "insufficient." The government further requested for an in-person interview with staff about the hacking. Then, Washington conducted a strict scrutiny assessment for his business. They assessed his processes, documentations, security protocols and trainings for the employees to ensure data protection. (NOTE: That's why we have made these assessments as our service)

Days of personal roller coaster turmoil passed by, and then his employees blamed him for the tragedies that happened. The employees left and searched for another employer not under government scrutiny and can give them better job security. Daugherty lost large amounts of clients as many of them switched to other providers. Insurance companies refused to renew his coverage.

Multitude of documentation was demanded from him by the FTC, together with countless requests for interviews and data that he had already provided. It took a great toll on him financially, emotionally, and mentally. Huge amounts of time and money were wasted. Paying for attorney's fees drained him and in the end he declared insolvency. The only things he was able to save are those what we have in his garage today.

Have you ever said, "It won't happen to me" or "Not to my company...?"

Never subscribe to the idea that you are safe from cyber-attacks because you are not a major corporation like Experian, J.P. Morgan or Target. Never lose your vigilance just because you have a "great" IT department and securities set-up.

Try not to believe you're in peril since you're "little" and not a major organization like Experian, J.P. Morgan or Target? That you have "great" individuals and securities set up? That it will not occur to you? -- This is PRECISELY what hackers want you to become - to be complacent, to subconsciously rest on your cyber security laurels so you become their easy victim.

According to an independent IT-security organization, there were 1.13 billion malware programs out there last 2020, and even more are present now. Small private companies are the target of 70% these cyber crimes (source: National Cyber Security Alliance); you may have not heard of these in the news simply because news agencies are only interested on BIG breaches OR that

hacked companies just wanted it to die down so their public perception won't be notoriously battered, avoid suits and shame.

But without a shadow of doubt, reality is - "small and ordinary" businesses are exposed to these business-killing threats every day, and stubbornly embracing this mindset of "That will not occur to me" is a surefire approach to leave yourself totally open to these cyber criminals.

The National Cyber Security Alliance revealed that one in every five small businesses have been victims of cybercrime last year - and this figure only states those that were reported. Meaning, many are still hiding their facts on cyber hacking because of the bad reputation and negative light that it will shed against their business. So it's safe to say that the number of small businesses compromised by cyber-attacks is higher than 20%.

The AVERAGE ransomware request is currently at $84,000 as per Osterman Research and more than $100,000 are lost per ransomware incident and over 25 hours of downtime.

Do you think you will always be "too small" and "out of the radar" of cyber criminals that they won't target you for ransomware? If they succeed, they will hostage your data for days and make demands.

Again, do you think you will be "too small" that cyber criminals won't install malware and use your server to illegally hold the data of your customers, vendors, employees? Do you think that hackers will think of you as unimportant that they won't illegally control your bank account?

The AVERAGE ransomware request is currently at $84,000 as per Osterman Research (source: MSSP Alert), and more than $100,000 are lost per ransomware incident and over 25 hours of downtime. Obviously, $100,000 isn't the apocalypse, right? In any case, would you say you are OK that this will happen? Will you take that risk?

It's not just the Cybercriminals who are the Problem - Unequipped Employees too!

Hackers from China or Russia are the common culprit in the minds of money when it comes to cybercrime; however, another equally dangerous "hackers" are disgruntled employees, either from your company or your vendors. Because of their insight into your system and access to your records, they can cause huge damage.

WHAT HARM WOULD THEY BE ABLE TO DO?

Confidential Business Information. They leave the company together with YOUR confidential business records and client data - these can be stored in their personal devices, software or online accounts. They still hold access to cloud applications, for example, online media and document-sharing platforms (Dropbox or OneDrive, for instance) that you're not even mindful they were using.

Osterman Research, in its comprehensive investigation, found out that 69% of business owners experience data disaster because of employee turnover and 87% of representatives who leave take

confidential information with them. How would they abuse that data? Offer it to contenders, BECOME a contender or hold it to use at their next work.

Stolen stocks, funds, client lists. Statistic Brain Research Institute, found that 75% of employees have stolen something from their bosses in some way. Employees use subtle ways to steal items such as inventory, credit card charges, or checks. Your hard-earned goes down the drain that you won't be able to recover. This occurs to many businesses and not a lot would want to admit.

The AVERAGE ransomware request is currently at $84,000 as per Osterman Research and more than $100,000 are lost per ransomware incident and over 25 hours of downtime.

But here's the most widely practiced way of stealing: Stealing TIME. They squander long stretches of hours by charging time against your hard-earned money where, in fact, they are actually doing personal tasks, play mobile games, mess around, shop around, soak in social media, gamble, read the news, and a LENGTHY list of non-business-related activities.

Your company when employees log time falsely. Instead of benefitting from the productivity of the 40-hour work week, you're paying more with less services. Some may even grumble about being "overloaded" and "exhausted" or demand that "You need to hire more staff!" so you do. Once permitted, this activity will suck your profits meant for growth.

We do put web security filters in employees' computers to limit the websites they visit. If not, they could do things that will put you in legal peril, such as downloading pirated music and videos, visiting adult-content sites, gaming, and gambling – all these websites belong to a HIGH-RISK category. These can transmit viruses, ransomware and cause cyber-attacks. The good thing, we presently have services to prevent employees from doing these risky activities).

Disgruntled Employees Delete EVERYTHING. A typical situation: A worker is terminated or stops since they are discontented with how they are being dealt with – however before they leave, they delete ALL data that they can get their hands on. Regardless of whether you sue them and win, the litigation expenses and squandered time for the purpose of recovering information, not to mention the mental burdens of it all, are far greater expenses than what you might get if you win the case.

Good thing, for our managed IT clients, we use data recovery and business continuity tools to keep business going; however, for customers who are not under this solution, they are helpless against this.

Are you *safe* from these hacking possibilities?

Loss of valuable data or money through unauthorized access. Data theft may be committed by your finance, HR and accounting who have special access to highly confidential data. Unauthorized extortion can be done not just by the leadership, but their staff or vendors. They can take cash or confidential information. One move regarding human resource can lead to great compromise - hiring an intern, part-time workers, or outsourcing to a vendor - some ill-minded person could abuse this access and sell data to third parties or channel funds from your account.

Unauthorized extortion can be done not just by the leadership, but their staff or vendors.

WHAT DO OUR OTHER CLIENTS SAY?

"The response time of the Troinet team is amazing! During the most recent storm (Isaias), our Eltingville office lost most of its power for several days. Our server connection was initially lost, and we were in a panic! Troinet worked quickly to get our server up and running and we were able to use the power we had to connect to our scheduling software. This permitted us to contact our patients and alert them of our situation and reschedule their appointments. Troinet sets the standard in efficient, responsive and professional customer service!"

Richmond Dental
Disaster Recovery

5 WAYS HOW CYBERCRIME CAN DESTROY YOUR BUSINESS

Clients who avail our IT Security solution can be assured that they will enjoy lesser cyber security attacks and their serious effects upon network compromise. But you should also know that there is definitely no 100% assurance you will not get compromised – you can just set up extraordinary protections that will decrease the odds of cyber theft, secure data and make it recoverable, and show your team, customers and legal officers that you WERE responsible and not negligent.

Realize that we are systematically assessing ALL our customer network systems and recommend NEW protections that we think you should set up.

1. Reputational Damages: What's more reprehensible than a cyber-attack? Attempting to cover it up. Companies like *Yahoo!* discovered this lesson in a difficult way. When they knew about the hacking, they DID NOT promptly disclose it to their clients, thus, they were confronted with multiple class-action lawsuits. Tools such as those used in the dark web can easily track the source where the data was stolen from. So, you cannot hide a cyber theft.

When hacking occurs, do you think your customers or patients will give you consolation? Have compassion? News will break out fast and non-parties may feast on it especially in social media.

When hacking occurs, do you think your customers or patients will give you consolation? Have compassion? News will break out fast and non-parties may feast on it especially in social media. Clients will be disgruntled and will insist for answers: "Have you been responsible? What protections did you put into place (Which we outlined in this article)? Or you will just tell your customers, "Sorry, we think this kind of cyber hacking won't happen to us," or "We don't want to spend extra cash." These are not enough to appease them.

2. Government Fines, Legal Fees, Lawsuits:

Most of lawmaking activities today revolve around data security. The government is enacting and enforcing more stringent guidelines and imposing heavier penalties on computer breaches. The courts DO NOT FAVOR you if you compromise customer data.

Don't assume that this only applies to large businesses: ANY private enterprise, whether big or small, that gathers client data will be obliged to inform clients in case of cyber compromise. Truth be told, 47 states and the District of Columbia each have their respective data breach statutes – and they are getting severe through time.

In case you are a healthcare of financial services provider, you have extra obligations under the Securities and Exchange Commission (SEC), Health Insurance Portability and Accountability Act (HIPAA), and the Financial Industry Regulatory Authority (FINRA).

ANY private enterprise, whether big or small, that gathers client data will be obliged to inform clients in case of cyber compromise.

In case you are in medical care or financial service industries, you have extra notice prerequisites under the Health Insurance Portability and Accountability Act (HIPAA), the Securities and Exchange Commission (SEC) and the Financial Industry Regulatory Authority (FINRA). In addition, HIPAA specifies that if a medical-related business encounters a data breach above 500 clients, it should inform a media agency about the occurrence. The SEC and FINRA likewise require financial service providers to reach them about cyber-attacks, like any other government agencies.

As an IT consultant and provider, we make sure that our clients stay compliant and have the proper protections in place.

3. Expenses, Damages, and Avoidable Losses:

A single ransomware attack, data hack, or rebellious employee can cost you unnecessary expenses, damages, and losses which could have been prevented in the first place. On top of that, there are operations interference, network downtime, delays, and piling of work. Loss of deals. Investigation and legal fees will devour your income just to figure out what sort of breach occurred and what information were compromised. IT restoration costs, if possible, to put back your operations again.

The assessed cost per stolen client record ranges between $150 to $225 each.

Cyber hackers may demand ransom from you, usually through a cryptocurrency deposit, and maybe - just maybe - you will get your data back. Then, there are expenses for litigation, attorneys, and expenses for reaching to the media. Your income will be deeply disturbed, and financial structure will implode. A few states give compromised businesses mandatory credit-observation for a year and expect that more entities will follow accordingly.

The assessed cost per stolen client record ranges between $150 to $225 each. This is after IT recovery, lost income, downtime, fines, and legitimate charges are computed. How many employees and customers do you have? Multiple that by $50 on the conservative side and you'll begin to get a feeling of the damages that a breach can bring to your organization. (Note: The highest cost per data breached belongs to the healthcare industry)

4. Bank Data Breaches: If your bank deposits were hacked, the bank is NOT liable by law to reimburse you. Here's the true story of Verne Harnish, best-selling author and CEO of Gazelles, Inc., a prominent and notable counseling firm. One of his famous books is The Rockefeller Habits.

A True Bank Hacking Story Where the Money was Never Returned

Do you keep rehearsing in your mind, "NOT ME, NOT my business, NOT my employees?" In the same principle, nobody believes they will be in a car crash when they leaf their house each day, and yet they put the safety belt on.

Hackers were able to access the PC Harnish, intercept the email correspondence with his assistant, and stole a whopping $400,000 from his account. The hackers, believed to be from China, tricked Harnish's assistant telling her to send money to 3 different locations. For the assistant, it was all a normal procedure since she was tasked to actively assist in financing a number of real estate ventures. Communicating under disguise, the hackers assured her that they are "Mr. Harnish" until she ultimately agreed to wire the funds. The hackers proactively erased the bank alerts sent automatically to the owner. Harnish also didn't notice them because of his tight work schedules. He wasn't able to get that money back, and the bank was not responsible and was legally-protected.

Do you still believe that one single is not capable of one single error that could compromise the whole organization? Do you keep rehearsing in your mind, "NOT ME, NOT my business, NOT my employees?" Can one small poor decision take away all of what I built for? **In the same principle, nobody believes they will be in a car crash when they leaf their house each day, and yet they put the safety belt on.** You don't anticipate a deadly accident everyday, yet you still put your seatbelt on. *What if*?

5. Using YOU to Breach Your Clients. Some programmers won't steal your money or hostage your data for ransom. There are some that will take advantage of the vulnerabilities of your network, server, or website to spread viruses to and compromise your clients. Once they hack into your system, they can use it to transfer spam, launch ransomware, develop bots, build link farms, or promote their political or religious agenda. This is also why it is better to install web gateway security, spam filtering, endpoint security, SIEM (Security Information and Event Management), and other items we detailed in this article.

HERE ARE OUR RECOMMENDED CYBER SECURITY SOLUTIONS

We Think All Clients Should Have in Place

For enhanced security, we suggest the following solutions to all our customers ASAP. We regularly update, launch better tools, procedures, and documentation, and will be sharing these as they become available.

Vulnerability Assessments and Quarterly Business Reviews (QBR)

We plan and hold these meetings with our clients. During these assessments, we run through some hazard appraisal activities and give you a score. We will likewise evaluate your feedback of our current service if there is such, survey your IT goals and financial plans, give an overview of our NEW solutions that we feel you may need. Then we make the proposal.

We offer complementary consultation which shall be FREE or absorbed into the execution of the service

We will likewise address any inquiry you have and ensure you are happy with our process. We also offer complementary consultation which shall be FREE or absorbed into the execution of the service.

Dynamic Security Monitoring, Patching

This is the main component we offer in our Managed Cyber Security Services Plan. We keep a proactive network security supervision to prevent problems from happening in the first place. When questionable patterns take place, we provide the remedy right away.

Insurance Review: At least once every year, we furnish a copy of our services and protections to YOU.

We can also work with your insurance specialist to audit your digital risk exposures, protections, and leverages. We may also look at your other policies to guarantee that we satisfy your overall requirements.

We want to reduce the pressure and stress of our clients in preventing and dealing with cyber-attacks

[NEW!] Data Breach and Cyber-Attack Response Solution

With this service, we want to reduce the pressure and stress of our clients in preventing and dealing with cyber-attacks. Overall, this can save precious time and money. Here, we work with our customers to customize and maintain and digital-response plan so that IF breach occurs, we could minimize the damages and keep the operations going. We then create an investigation process to avoid reoccurrence.

Ransomware-Proof Backup and Cyberattack Recovery Plan

Cyber criminals are aware that you have backups, so they design their assaults to RUIN your BACKUP documents too. This is the reason we are demanding customers to avail our Upgraded Backup Solution, which is a part of our Managed Services Plans.

Security Policy for Mobile and Remote Devices

All gadgets used remotely - from PCs to mobile phones - should have regular back up. program and have a remote "factory reset" switch that would wipe the information from a lost or taken gadget. You also must have a program to manage what employees can and cannot access in the company-owned devices. They should be trained who to utilize these remote devices responsibly and how to respond if it is lost or stolen.

Develop Strong Company Password Practices

Are your employees' passwords strong enough? STILL, one of the greatest dangers to businesses are WEAK passwords. To protect you against this, we require employees to follow the best practices in password management and incorporate strategies to ensure that weak passwords are never used. Here are some:

1. Prohibit the use of the most common passwords. We start with the most commonly hacked words.
2. Send alerts to users for strange log-in attempts.
3. Install an auto-lock mechanism for multiple failed attempts.
4. Train employees how to create strong passwords and manage them well
5. Keep software updated to ensure latest security updates are installed

Multi-Factor Authentication (also called MFA, 2FA)

We recommend 2FA if we see that a certain process involving a device, website or application this extra layer of security. The access will be successful upon presenting two or more pieces of factors (or evidence) from a user's given devices.

Web Content Filtering

This is a part of web protection features that enables your organization to track and regulate access to websites based on their content classifications.

The top categories searched on the internet are still porn, online gambling, and file-sharing sites for those who don't want to pay for a movie, song, or software. These websites are dangerous because attackers may include spyware, viruses, and worms into the files.

When harmful files are downloaded from questionable websites, your company computers will be infected which you surely don't want to happen. These could expose your business to lawsuits and fines - not to mention the money and time wasted on unproductive employee behavior.

When these files are downloaded, your company computer becomes infected which you surely don't want to happen. Illicit online activities, sexual harassment, or child pornography are some of the things that can be done with the work laptop and could expose your business to lawsuits and fines - not to mention the money and time wasted on unproductive employee behavior.

[New!] Cyber Security Training for Employees

Those who aren't equipped may open an email and attachment without suspecting that such email was infected by a spyware.

Your employees need REGULAR online cybersecurity training to protect themselves and the company against cyberattacks. Security-savvy employees are your primary defense against hacking.

Those who aren't equipped may open an email and attachment without suspecting that such email was infected by a spyware.

A popular tactic among hackers is to incorporate a malware into a malicious file from unsecured sources. Once it is downloaded by an employee, it can give the hacker complete access to your

device, and even the whole network. Yes, you may have firewalls in place, but they're just not enough. Employees are the most common entry points for '*phishers'* and investing in their cybersecurity training is one of the best decisions you can make. We provide basic training for this. For example, we educate them how to identify spam content that could be hiding malicious software. The training also includes awareness of the dirty tricks that lead employees to download ransomware, or 'social engineering' mechanisms that fake trusted online identities.

Maximize Confidentiality of Emails

Employees may send sensitive or confidential company information and documents. Some industries like those in the healthcare service are required to protect their client's sensitive information.

It is a must for employees to know how to secure confidential documents before send the email.

It is a must for employees to know how to secure confidential documents before send the email. We both train employees and arrange email systems to maximize confidentiality in sending or receiving sensitive data.

Secure Remote Access Activities

Using remote access tools such as TeamViewer, Anydesk, Remote Desktop pose data security threats to your business.

It brings convenience by enabling other users to access from a remote location, but one wrong move can cause your network to fall into the wrong people. Once they gain access, they can cause data theft or deploy ransomware.

To mitigate the risks, we introduce solutions such as using a business-grade VPN, limiting long-term access, or introducing reliable intrusion detection systems (IDS) and Intrusion Prevention Systems (IPS).

To mitigate the risks, we introduce solutions such as using a business-grade VPN, limiting long-term access, or introducing reliable intrusion detection systems (IDS) and Intrusion Prevention Systems (IPS).

[New!] Dark Web Scan and Monitoring

Your personal information and credentials, if compromised, may be sold or traded in the dark web. Without knowing, it may be too late to discover that your crucial business documents and private files have been compromised.

We provide you with proactive tools and training so you can properly respond when dark websites compromise you.