The Cybersecurity Challenge

Urgent and critical protections we are urging all of our clients to Have In Place NOW to protect their financials, data, productivity, confidential information, and reputation from the Tsunami of Cybercrime rampant in today's environment

The growth and sophistication of cybercriminals, their ransomware and hacker attacks continue to increase at exponential levels, and NEW protections are now required to be prepared to address these threats.

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.

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

By Michael Moran, President Affiliated Resource Group
5700 Perimeter Drive, Suite H-Dublin, Ohio 43017
Visit www.aresgrp.com or Call 614-495-9658

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

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, 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…

Ohio has Data Protection law that requires organizations to notify individuals (Ohio residents) whose specified Personally Identifiable Information (PII) have been involved in a data breach within 45 days of realizing they have had a breach that their information has been compromised and potentially been exposed to cybercriminals. Other states notification period is as little as *three (3) days*.

65% of respondents in a recent national survey said they would seriously consider alternatives to a health care provider if they knew the provider had suffered a data breach….

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.

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

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. Ransomware payments increased over 184% between quarters in this past year alone. This is very alarming.

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 "we're too small", "we've got it covered"* 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 5 years ago, BUT NOT TODAY.

Consider the story of the Brookside ENT Medical Practice, which has now permanently closed its doors.

Ransomware encrypted the system at Brookside ENT and Hearing Center in Battle Creek which housed patient records, appointment schedules, and payment information rendering the data inaccessible. The attackers claimed to be able to provide a key to unlock the encryption, but in order to obtain the key to decrypt files, a payment of $6,500 was required.

The two owners of the practice, William Scalf, MD and John Bizon, MD, decided not to pay the ransom as there was no guarantee that a valid key would be supplied and, after paying, the attackers could simply demand another payment.

Since no payment was made, the attackers deleted all files on the system ensuring no information could be recovered. The partners decided to take early retirement rather than having to rebuild their practice from scratch.

The FBI was alerted to the security incident and explained that this appeared to be an isolated attack.

But lacking any medical and billing records, the doctors closed the business retired over a year early and lost a valuable asset in their practice and patient records. Patients who had not obtained copies of their medical records prior to the ransomware attack lost all records stored by the practice.

"There was no way to communicate the closer to the patients; we didn't even know who had an appointment in order to cancel them" one of the doctors said. "So I just sort of sat in the office and saw whoever showed up for the next couple of weeks and told them the news."

"Not My Company-Not My People-We're Too Small"

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: 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 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?

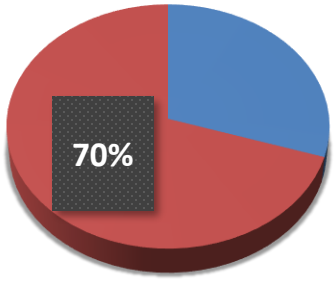
Are you "too small" to deal with a hacker using your company's server as "ground zero" to infect all of your clients, vendors, employees and contacts with malware? Are you "too small" to worry about someone taking your payroll out of your bank account? According to Osterman Research, the AVERAGE small 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?

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 a majority of hacks and breaches are "facilitated by employees. As proof, a recent Forrester study about internal threats found that:

- ***About 1/3 of all security breaches*** **stem from lost, stolen, or non-maintained devices** that took too long to discover were missing; were not patched/updated properly.

- ***27% of breaches are caused by inadvertent misuse of data*** by employee's vulnerabilities in some form (they inadvertently provided their credentials to the hacker/malware)



- ***An additional 12% of breaches are caused by malicious insiders***, most of whom were never suspected of "*being the type*."

- ***So, up to 70% of security breaches could be prevented*** with improved training, better IT operations management, and processes to manage system and data access.

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

We regularly speak at industry conferences about improving your cybersecurity programs and hear stories from attendees about how a trusted member of the staff got fooled into doing something wrong by a phishing email or vishing phone call that either compromised their credentials to the criminal or wired money to a nonexistent vendor – sometimes tens of thousands of dollars – *and many of these are small organizations*.

If you think you are safe because your systems are in the cloud, think again. Recently, a Central Ohio on-line product-launch company with hundreds of clients, was hacked, erasing or corrupting files representing years' worth of work for clients and leads databases that were all hosted in the cloud. "There was millions of dollars in damage done to the company; worse, clients businesses at least temporarily went offline too. Client's complete app businesses were wiped out by this," the owner said. "That's one of the hardest parts about this." He had to close his business of 12 years.

AFFILIATED
Cybersecurity, Compliance, & Managed IT Support

Exactly How Can You Be Damaged By Cybercrime?
Let Us Count The Ways…

IMPORTANT: Clients who work with Affiliated DO have a number of 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! And many others are learning that lesson the hard way, facing multiple class-action lawsuits for NOT telling their customers 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 or patients will rally around you? Have sympathy? News like this travels fast on social media. They will demand answers:

   HAVE YOU EXERCISED RESONABLE DUE CARE TO PROTECT MY DATA?

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.

3. **Don't think for a minute that this applies only to big corporations:** ANY organization that collects Personally Identifiable Information also has important obligations to those people to tell them if they experience a breach. In fact, almost every state and the District of Columbia each have their own data breach laws that cover their residents (and you are responsible if you capture their information) – and they are getting tougher by the minute.

   Healthcare, financial services, and federal government clients have 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), and the NIST 171-800 requirements.

   Each have a number of rules, specifications, and reporting requirements for the protection of protected information. Additional security processes and monitoring tools for anomaly detection are part of the requirements for these industry groups. 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 discuss with our clients who have Quarterly Business Reviews (QBR's) as a part of their agreements is how to ensure you are working toward compliance providing a reasonable level of due care over the data that your collect and manage.

4. **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: Healthcare data breach costs can be as high as $400 per record.]

5. **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?*

6. **Using YOU As The Means To Infect Your Clients:** Some hackers don't just lock your data for ransom or steal money. Often, they use your server, website or profile to spread viruses and/or compromise other PCs. They send e-mail form you (spoofed from you) and send ransomware to your contact base. If they hack your website, they can use it to relay spam, run malware, build SEO pages or promote their programs and your clients become next level victims.

Affiliated's Recommended Protections
You Should Have In Place Now

Below is a list of things we recommend all clients have in place for their security, based on your specific needs and regulated industry requirements. **Some you may already have, and some may be lacking, which is why we are conduct regular reviews with our clients to evaluate their current situation and make suggestions for ways to address any exposures or areas for improvements.**

We are also working to continuously review and implement new tools, protocols and processes, to stay current with the ever-evolving regulations and threat landscape; we share these offerings and updates with our clients as they come available, and in our reviews and as a part of our annual agreement renewals.

Base Level Security Services

☐ **Proactive Monitoring, Patching, Security Updates:** This is what we deliver in our base Full Managed IT Services and Managed Infrastructure Services Plans. Specifically, we monitor your systems, ensure workstations and server operating systems are properly patched, Anti-Virus is up to date, and maintenance is done to the firmware on your devices to keep them current to manufacturers requirements via our PIM process.

☐ **More Aggressive Password Protocols:** Employees choosing weak passwords are STILL one of the biggest threats to organizations. To protect against this, we implement password policies that require password changes for all employees and put in place controls to ensure weak, easy-to-crack passwords are never used and that passwords cannot be reused for a period of time. We will also have checklists for employees who are fired or quit to shut down their access to critical company data and operations].

☐ **Cybersecurity Awareness Training Program:** Employees accidentally clicking on a phishing e-mail or downloading an infected file or malicious application accounts for 27% of the way that cybercriminals hack into systems. Training your employees FREQUENTLY is one of the most important protections you can put in place. Seriously. Our PROGRAM informs and reminds and incents your employees to be on high alert and reduce their likelihood of clicking on the wrong e-mail or succumbing to other scams.

☐ **Compromised Credentials 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 adjust your accounts and be on high alert.

- ☐ Utilization of Current Generation **Intelligent Firewall Protection**: Utilizing the features of the current generation of intelligent firewalls will provide significantly more security protection that than the previous "hardware" based systems. Having the ability to update software to add features and functionality that can be layered to provide better threat protection.

- ☐ Appropriate Group Policies for **User Access Control** over sensitive data and systems

- ☐ **Insurance Review:** At least once a year, we will provide you with a copy of our policies and protections 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.

- ☐ **Annual Network Security Risk Assessments (NSRA):** we can provide an annual NSRA based on your organizations needs to ensure that you are protected and are secure. Over the course of the year, many organizations, especially those with internal IT staff teams, adjust and implement new systems in their IT environments – affecting their security. In addition, new threats and exposures are constantly being created. This process can also validate that your cyber insurance policy is in compliance.

- ☐ **QBRs Or Quarterly Business Reviews:** We will be more persistent in scheduling and holding these meetings with all of our agreement clients. During these consultations, we will discuss a security risk reviews and assessments and provide you with a score. We will also brief you on current projects, review your IT plan and budgets, discuss your business goals and plans to ensure that your IT resources are secure and aligned with your goals. We will also answer any questions you have and make sure you are satisfied with our services.

Advanced Security Protection

- ☐ **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. While that is not true, we are also recommending clients also include our advanced endpoint security solution to monitor and address behavior and activity based events that those that wish to do harm use to access and propagate your systems.

- ☐ **Multi-Factor Authentication:** Depending on your situation, we will be recommending multi-factor authentication for access to critical data and applications; even accessing your initial windows sign on.

- ☐ **Protections For Sending/Receiving Confidential Information Via E-mail (encryption):** Employees have access to a wide variety of electronic information that is both confidential and important. That's why we'll be ensuring specific clients' e-mail systems are properly configured to prevent the sending and receiving of protected data.

- ☐ **Incident (Data Breach And Cyber-Attack) Response Plan:** This is a time- and-cost-saving tool as well as a stress-reduction plan. We have an internal response plan for addressing the technical steps in a response; we will be working with our clients to create and maintain an overall cyber-response plan so that IF a breach happens, you 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 is one of the reasons why we are recommending our clients upgrade to our managed backup solution, which is included in our MBDR Managed Data Agreement.

- ☐ **Ongoing Securing Programs (OSP)**: Our OSP is a solution designed to meet the specific needs of clients based on their risk management and regulatory requirements. We have the abilities to provide quarterly scans, enhanced endpoint protection, incident planning and event Security Incident Event Management systems (SIEM) to assist with regulatory requirements for monitoring of systems and Microsoft logs.

- ☐ **Mobile And Remote Device Management:** All remote devices – from laptops to cell phones – need to be managed. 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.

Our Preemptive No-Obligation Cybersecurity Risk Review Will Give You The Answers You Want, The Certainty You Need

On our own initiative, we will conduct a thorough, CONFIDENTIAL review of your systems and environment, backups and security protocols as outlined in this report and generate a custom "Risk Review 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, industry, etc.

We will be sharing your Risk Review Health Score, during your scheduled operations review meeting.

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 meeting (if appropriate).

If you have any questions, **call your account manager at 614.495.9658 or send me an e-mail michaelmoran@aresgrp.com and I will be happy to help answer your questions.**

We know you are *extremely busy* and there is enormous temptation to discard the warnings around cybersecurity, 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 WE can guarantee:** At some point, you will have to deal with a cybersecurity "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, we can practically guarantee this will be a far more costly, disruptive and devastating disaster.

You've spent your career working hard to get where you are today. Let us help you prepare to avoid a potential big bump in the road and give you complete peace of mind.

Dedicated to your success,

Michael Moran
President

Here Are Just A Few Other Clients We've Helped

Affiliated Provides Experienced Strategic IT Planning for Secure Growth

The single biggest benefit of working with Affiliated has been their ability to help with strategic planning for our security and growth. From setting the strategy with our IT team, to coordinating security programs and processes, facilitating hardware and software purchases, to collaboration on projects and troubleshooting issues, they bring a high level of experience to every facet of our IT eco-system. And because the entire Affiliated team has taken the time to understand our business and needs; they have been critical to our success in aligning our IT department's goals to our overall company goals. It is a strong partnership and has been for 10 years. — ***Craig,*** *CFO, Buckeye Power Sales*

For More Than 20 Years Affiliated Has Been our Trusted Advisors, Kept Our Team Productive, Systems Running, Secure, and Compliant

"The team at Affiliated has worked with ABITEC for over 20 years. They've kept our systems current, secure, and our team productive. They have advised us correctly on a variety of topics ranging from strategic IT planning, application selection and support, Disaster Recovery options and plans, remote facility management and network building, global integration, and compliance activities to meet our global and corporate auditor's requirements. Even after our parent organization decided to absorb all of our IT infrastructure into a centralized support center, we continued to rely on Affiliated for advice and guidance. They are a great partner and I would recommend them to anyone who needs a professional, trustworthy team to support them." —***Brad,*** *CFO, ABITEC*

Affiliated Has Helped ASNT Advance And Secure Our Systems; Their Support And IT Guidance Is Well Worth The Investment

"Affiliated started providing our association with a variety of projects that we needed for IT. As our needs increased, they recommended their Managed Services program and are we glad we chose it! They provide me with a trusted resource to develop and review my IT strategy quarterly, design, implement and support our organizations protection and the security practices that match our leadership teams risk expectations, projects that we need in a timely and cost-effective manner, ensure we are secure, provide User Security Training programs, and provide our users get the support they need in a responsive manner. Their leadership is always available in case I have a question or need assistance and their daily communication and support allows me and our team to focus on serving our members and the association around the world. We appreciate and have a great relationship with Affiliated*." —* ***Mary,*** *CFO, ASNT*