motiva

6 CRITICAL FACTS EVERY BUSINESS OWNER MUST KNOW ABOUT THE NY'S SHIELD ACT: DATA BREACH NOTIFICATION LAW

The SHIELD Act requires that businesses set up a "Data Security Program" to monitor and improve cybersecurity. Businesses must also implement "reasonable safeguards" to ensure that private information is stored and erased safely. The Act requires businesses to notify their customers of data breaches, and it imposes large fines if they fail to do so.

Provided by Walter Contreras, CEO of Motiva I Motiva.net I 646-374-1820

A LETTER FROM THE AUTHOR:

WHY WE CREATED THIS REPORT AND WHO SHOULD READ IT

Dear Colleague,

Back in the spring of 2019, the New York legislature passed Senate Bill 5575, the Stop Hacks and Improve Electronic Data Security Act, aka the SHIELD Act. The SHIELD Act impose specific cybersecurity requirements on businesses. The Act says that in order to achieve compliance businesses that own or license computerized data that includes "private information" of New York State residents must implement a "data security program".

That's why we wrote this report. We wanted to give CEOs and CFOs a simple, straightforward guide that not only answers your questions in plain English, but also provides vital experience-based information that most IT companies don't know (or may not tell you) about being in compliance with the new Cybersecurity Regulations.

My name is Walter Contreras, we are a local Cybersecurity and IT Managed Services provider on Long Island for over 15+ years. Our experience with Technology and how this affects the way organizations do business gives us an inside knowledge of how Cybersecurity Regulations represent a shift from the traditional way of thinking about IT resources.

The simple fact is, the NY Shield Act applies to any business that holds private information of a New York resident – as well as non-public information, regardless of whether that organization does business in New York – if you fail in fulfilling the requirements to comply with the law, you may be subject to liability, and hefty fines.

Of course, I am always available as a resource for a second opinion or quick question, so please feel free to contact my office direct if we can clarify any points made in this report or answer any questions you have.

Dedicated to serving you,

Walter Contreras,
CEO at MOTIVA

motiva

ABOUT THE AUTHOR

Founder and CEO of Motiva Networks since 2007, Walter brings more than 25 years of Technology Industry Leadership in Cybersecurity, and Software Development.

Walter oversees the corporate direction and strategy for Motiva's operations, including sales, support, consulting, marketing, and partners. He focuses on strategy, leadership, innovation, and clients. "It's our duty as an organization to empower Small Businesses, with tools and innovation second to none. So that they too have a chance to succeed as a global member of the business community".

Before creating Motiva, Walter worked at NSLIJ Health System as a Support Engineer, and it was there that he was truly inspired to help others.

With Walter's vision. Motiva has expanded their IT Services, from the traditional model to something unique where Cybersecurity is paramount "Every business is different in itself and we adhere to their needs not ours". Motiva's services expand from Cybersecurity and Compliance, 24/7 Help Desk, Software Development, VoIP and Disaster Recovery Solutions".

Walter is a graduate of Columbia University Business School and holds several certifications on his field.

"Our Mission is to serve and support our customers to the best of our abilities. And to help develop their businesses through the innovation of technology".

THE SHIELD ACT: WHAT YOU NEED TO KNOW ABOUT NEW YORK'S NEW DATA BREACH NOTIFICATION LAW

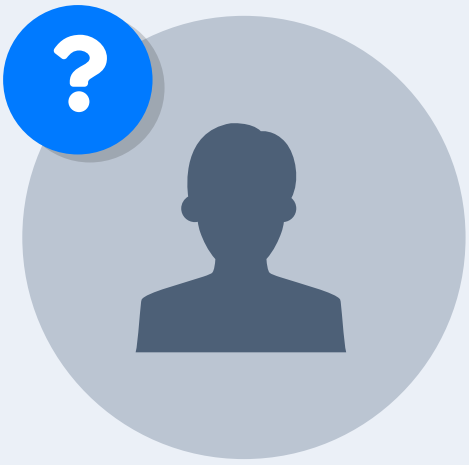
In this report I'm going to talk about very important facts you need to know about the **Stop Hacks and Improve Electronic Data Security (SHIELD) Act**. These include:

1. What is the SHIELD act?
2. Who does this law apply to?
3. What are the requirements and what I must do to comply?
4. Can my IT guy do it?
5. Penalties for Non-Compliance

WHAT IS SENATE BILL 5575?

Senate Bill 5575, more commonly referred to as the New York Stop Hacks and Improve Electronic Data Security (SHIELD) Act was enacted on July 25, 2019 as an amendment to the General Business Law and the State Technology Law updating the breach notification requirements to impose stronger obligations on businesses handling private information and personal information in an attempt to mitigate threats that contribute to identity theft.

New York State Senator Kevin Thomas said "It is critical that our laws keep pace with the rapidly changing world of technology. [T]he SHIELD Act...will allow for increased accountability and diligence in regards to consumer privacy. Now more than ever, it is important that businesses protect the private information of the consumers they serve."



HOW DOES THE NY SHIELD ACT DEFINE PERSONAL INFORMATION AND PRIVATE INFORMATION

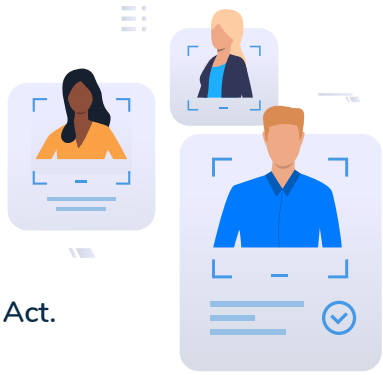
While the regulation defines "personal information" as "any data about a natural person that can be used to identify the individual, it defines "private information" as either personal information in combination with a variety of traditional non-public personally identifiable information or a user name/email address in combination with a password or security question/answer that permits access to an online account.

Continued from pg.3

The SHIELD Act defines private information data elements as:

- Social security number
- Driver's license number or non-driver identification card
- Account number
- Credit or debit card number in conjunction with:
  - Security code
  - Access code
  - Password
  - Any other information that permits financial account access
  - Account, credit card or debit card number if such number permits financial account access without additional identifying information
- Biometric information defined as data generated by electronic measurements of an individual's unique physical characteristics including but not limited to:
  - Fingerprint
  - Voice print
  - Retina or iris scan

EXPANDS SCOPE OF LIABILITY



Similar to the CCPA and the GDPR, the SHIELD Act expands liability to any organization that collects private information of New York residents, regardless of where it was collected. This means that an organization does not necessarily have to conduct business in New York in order to come under the purview of the SHIELD Act.

EXPANDS BREACH NOTIFICATION TRIGGERS

By expanding the definitions of "breach" and "private information," the SHIELD Act has significantly expanded New York's data breach notification laws. The expanded definitions, in effect, create more instances where a business would be required to notify New York residents of a data breach.

Under the SHIELD Act, a "breach" has been broadened from mere unauthorized acquisition to additionally include unauthorized access to private information. Unauthorized access can include viewed, communicated with, used, or altered by a person without authorization to do so.

As such, an event that would trigger a breach notification may not just result from someone unlawfully taking data, but also unlawfully seeing the data without ever having possession of it.

Continued from pg.4

"Private information" is a subset of personal information – or any information that can be used to identify a person. Before that included highly-sensitive personal information like Social Security numbers, credit or account numbers, and identification card numbers like driver's license numbers. Now, under the SHIELD Act, private information has been expanded to include any account information, biometric data (like iris scans, fingerprints, voiceprints, images, etc.) used to authenticate someone's identity, and usernames or emails in combination with passwords or passcodes.

New York's data and privacy laws require that in the event of a breach, the business must notify any and all New York residents whose private information may have been compromised. Now, with the expanded definitions of breach and private information, there is the potential for more events that will trigger New York's breach notification requirements. Further, with these laws applying to any business that has New York residents' information regardless of where the business is located, such breach notifications will apply to far more businesses and any breaches they may experience.

This, therefore, expands the potential risk of and liability associated with a breach.

REQUIRES ADOPTION OF DATA AND CYBERSECURITY POLICIES

In addition, the SHIELD act requires organizations to adopt "reasonable" security practices, policies and procedures to safeguard sensitive data in three critical ways: administrative safeguards, technical safeguards and physical safeguards. This includes implementing practices to identify and prevent risks to data security, taking reasonable steps to secure the business's facilities and premises, choosing vendors who also maintain reasonable data and security, and taking steps to reasonably prevent unauthorized access to sensitive data and other information.

Taking into account differing sizes and resources of businesses, the SHIELD Act emphasizes that the programs should be at a minimum, requires ongoing monitoring of the implemented policies and procedures, regular risk assessment of the business's technical infrastructure and physical premises, training personnel, reasonable vendor due diligence, as well as designating an individual responsible for the required policies, practices, assessment and maintenance thereof.

WHAT THIS MEANS FOR YOUR BUSINESS?

If you are already concerned with data privacy regulations, thekey is to review and reassess your data privacy policy and security practices in light of the expanded definitions of a breach and private information under the Shield Act and to be ready to notify the New York residents in your database in the event of unauthorized access to their Notice should be sent to those New York residents. The SHIELD Act does not, however, require additional notice if notice is already being provided under a separate similar privacy statute, like HIPAA, DFS, GDPR.

Continued from pg.5

Following notice, you may be subject to liability, but not directly from a New York resident. Unlike the CCPA and the GDPR, there is no private right of action and only the New York Attorney General can take an action against a company in the wake of a breach of the SHIELD Act.

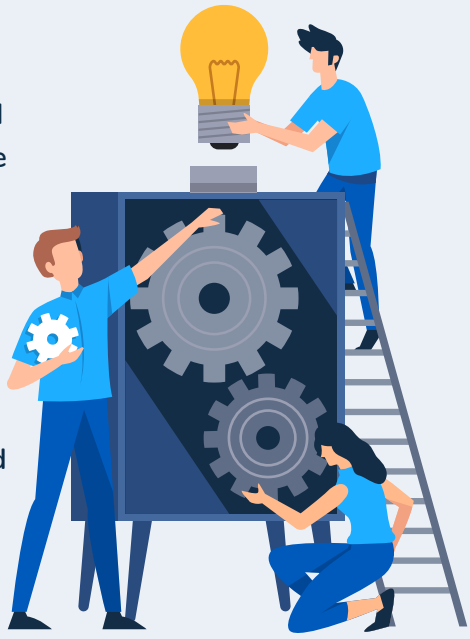
So while the SHIELD Act generally fits within measures that companies are taking for general data privacy and cybersecurity, particularly for GDPR and CCPA compliance, it is important to know that you may have special obligations to New York residents in the event of a breach and when a breach is considered to have occurred.

THE SHIELD ACT IMPOSES SPECIFIC CYBERSECURITY REQUIREMENTS ON BUSINESSES.

The Act says that in order to achieve compliance businesses that own or license computerized data that includes "private information" of New York State residents must implement a "data security program" that includes the following safeguards:

Administrative

- Designation of one or more employees to set up the security program
- Identification of probable foreseeable external and insider risks
- Appraisal of existing safeguards, workforce cybersecurity training, and
- Selection of service providers experienced in maintaining appropriate safeguards and requiring those safeguards by contract



Technical

- Risk assessments of IT network
- Information processing and software design
- Transmission and storage, enforcement of measures to detect
- Avert and respond to system failures, and regular testing and monitoring of the effectiveness of key controls

Physical

- Evaluate risks of information storage and disposal
- Identify, prevents and responds to intrusions
- Protects against unauthorized access to or use of private information during or after the collection, transportation and disposal of the information
- Properly discard private information within an appropriate amount of time after it is no longer needed for business purposes

PENALTIES FOR NON-COMPLIANCE

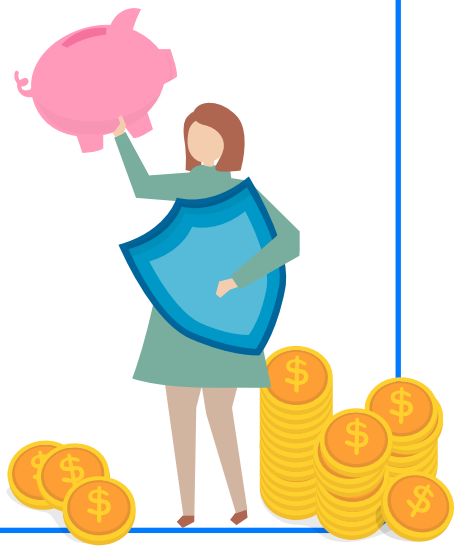
The SHIELD Act will be enforced by the New York Attorney General. The Attorney General can take action in court against a business if the business violates certain parts of the Act. As of the middle of 2019, the Attorney General's office has fined over $600M related to data breaches.

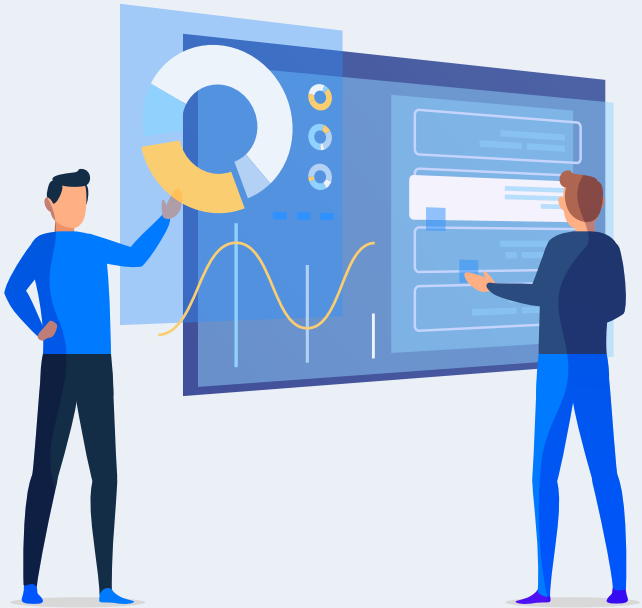
The Attorney General must act within three years of becoming aware of a violation (including where the business notified the Attorney General of the breach directly).

Fines can be issued under the Act issued where a business has failed to properly notify people affected by a data breach. The fines will be a civil penalty of either:

- $5,000, or
- $20 per violation (i.e., per person who was not properly notified of the breach), up to a maximum of $250,000

The Attorney General will issue whichever of these two penalties is greater.





PROVIDING NOTICE OF A DATA BREACH

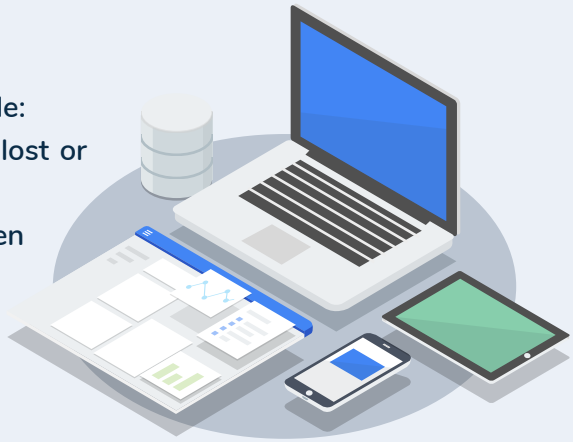
If a data breach occurs, the SHIELD Act requires a business to communicate directly with the people who have been affected by the data breach, and also to inform public authorities with the appropriate type of data breach notice.

What Counts as a Data Breach? Rather than "data breach," the SHIELD Act uses the term "breach of the security of the system." This can cover situations where a system has been compromised but it isn't clear whether data has been accessed or acquired.

Continued from pg.7

A data breach is where a person without proper authorization accesses or acquires computerized data. The computerized data could compromise the security, confidentiality or integrity of the private information of New York residents.

- "Accessed" usually means that there is some indication that the information has been:
  - Viewed
  - Communicated with
  - Altered
- Signs that information might have been "acquired" can include:
  - A computer or device containing such information is lost or stolen
  - There is evidence that the information has been downloaded or copied
  - There are reports of identity theft using the information



Access, in good faith, by employees of your business doesn't count as a data breach; unless there's some evidence that information was disclosed to an unauthorized person.

INDIVIDUAL NOTICE

There are several ways to give individual notice of a breach under the Act:

- Written notice
- Electronic notice, if the affected person has consented to electronic notice
  - A business cannot deny or withdraw service because a person has refused consent to electronic notice of data breaches
  - The Act distinguishes electronic notice from email notice. It may refer to notice via "push notification" or some other electronic notification method agreed between you and your customers
- Telephone notification, if you keep a log of the call

SUBSTITUTE NOTICE

There is also a list of substitute notification methods. You can only use these methods when one or more of the following applies:

- The cost of providing individual notification would exceed $250,000
- Over 500,000 people have been affected by the data breach
- You don't have contact details for the affected people

Continued from pg.8

The substitute methods of notice include:

- Email notice (if you have the consumer's email address)
    - You must not use this method if the breach relates to the security of email address or email account login credentials. In this event, you should set up a notification of the breach when the user logs into their online account.
        - This notification should only appear if the user logs in from an IP address or online location from which the user normally accesses the account
- Conspicuous notice via your website
- Notification via statewide media

WHAT INFORMATION SHOULD YOU INCLUDE WHEN PROVIDING NOTICE

Regardless of which type of notice you're providing, you must include the following information:

- Your company's contact details
- Telephone numbers and websites of state and federal agencies who can help with data breaches and identity theft
- A list of the types of data that have been (or may have been) accessed or acquired
- The specific elements of personal or private information that have been (or may have been) accessed or acquired

NOTIFYING THE AUTHORITIES

Whenever you have notified individuals about a data breach, you'll also need to notify these public authorities:

- New York State Attorney General
- New York Department of State
- New York State Office of Information Technology Services

If more than 5,000 New York residents have been affected by the breach, the SHIELD Act states that you must also notify "consumer reporting authorities." The Act doesn't specify which consumer reporting authorities you should notify. The Federal Government provides this list of New York State consumer protection offices.

Make sure that you prioritize giving notice to the individuals affected. Informing the authorities must not cause any delay to you informing individuals.

- You must tell these organizations
- The date(s) that you notified the individuals
- The content of your data breach notice
- How you distributed your notice

NOTE:
You must also provide a template copy of the notice you used.

EXCEPTIONS FOR CERTAIN TYPES OF BUSINESS

Some businesses will be deemed to be compliant with the SHIELD Act's data security requirements by default. They don't have to set up a data security program, and they don't need to implement the Act's reasonable safeguards.

However, they must still obey the Act's breach notification rules.

The Act calls such businesses "compliant regulated entities." Compliant regulated entities are already compliant with certain recognized data security standards. These regulations are as strong as (or stronger than) the standards set out under the SHIELD Act.

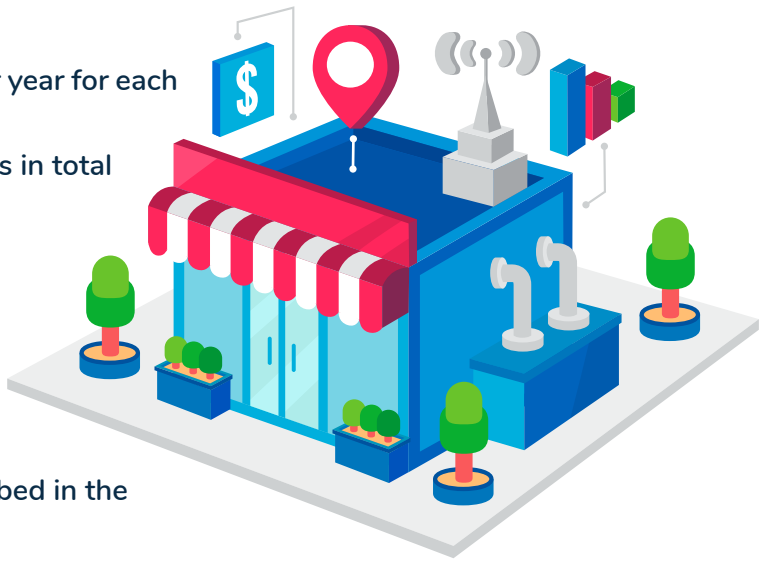
Compliant regulated entities are subject to (and compliant with) one or more of the following data security regulations:

- Section V of the Gramm-Leach-Bliley Act (15 USC § 6801 - 6808)
  - This mainly applies to financial institutions
- The Health Insurance Portability and Accountability Act (HIPAA)
  - This mainly applies to healthcare providers and health insurance companies
- Part 500 of Title 23 of the Official Compilation of Codes, Rules and Regulations of the State of New York (23 NYCRR 500)
  - This applies to financial services companies

SMALL BUSINESSES

The SHIELD Act applies differently to small businesses. The Act defines a "small business" as a business that:

- Has fewer than 50 employees
- Has had gross revenue of less than $3 million per year for each of the previous three fiscal years, or
- Has less than $5 million worth of year-end assets in total



A small business still needs to comply with the Act. However, there is some flexibility regarding the data security measures described in the "Keeping Private Information Safe" section.

There is no flexibility regarding the obligations described in the "Providing Notice of a Data Breach" section.

Continued from pg.10

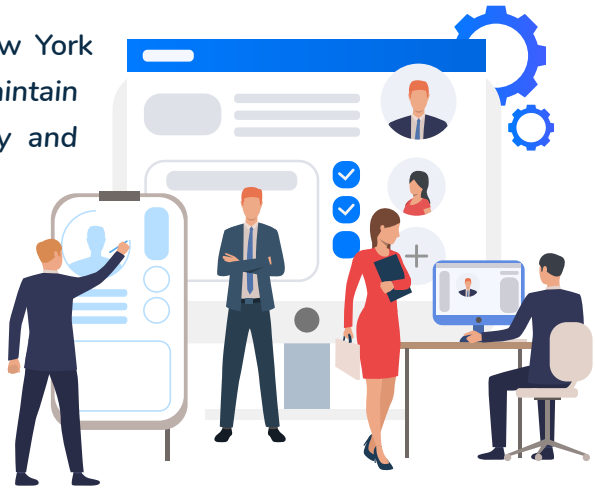
When implementing its data security program and reasonable safeguards, a small business only needs to take measures that are "appropriate," considering:

- The size and complexity of the small business
- The nature and scope of its activities
- The sensitivity of the personal information it collects from its customers

The SHIELD Act doesn't provide any specific guidance on what might constitute an appropriate level of data security for a small business. It's likely that this section of the Act will be considered by the Attorney General and the courts in the event of a data breach. Small businesses are unlikely to be held to the same stringent standards as larger businesses.

WHAT EMPLOYERS NEED TO KNOW

The SHIELD Act requires employers in possession of New York residents' private information to "*develop, implement, and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information.*"



The SHIELD Act does not mandate specific safeguards but instead provides that a business will "be deemed to be in compliance with" this standard if it implements a "data security program" that includes all of the elements enumerated in the SHIELD Act. Some key elements with relevance to HR stakeholders include the following:

- Designating an employee or employees to coordinate the data security program.
- Training and managing employees in the security program practices and procedures.
- Assessing internal and external risks and implementing controls to reduce those risks.
- Vetting service providers and binding them contractually to safeguard private information.
- Securely destroying private information within a reasonable amount of time after it is no longer needed for business purposes.

The human resources team can play an important role in each of these elements of a data security program. HR may need to ensure that employees designated to implement the data security program have the bandwidth to perform these responsibilities in addition to other assigned responsibilities.

Employee training typically is an HR responsibility, and information security training for line employees should focus on properly handling sensitive information, a natural topic for HR professionals.

Continued from pg.11

While risk assessments may focus heavily on technical threats, they also need to assess threats raised by negligent and malicious insiders. HR departments routinely outsource functions involving private information. HR professionals should ensure that those vendors' data security programs are properly vetted, and that legal counsel has included adequate information security terms in vendor agreements.

Finally, HR needs to ensure that records containing the private information of New York employees are securely destroyed promptly after the applicable retention period expires.

Two types of businesses can satisfy the "reasonable safeguards" requirement other than by implementing a data security program as defined by the SHIELD Act. Small businesses—those with fewer than 50 employees or less than $3 million in gross annual revenue—need only ensure that their data security safeguards are appropriate for the size and complexity of the small business, the nature and scope of the small businesses' activities, and the sensitivity of the personal information the small business handles.

Businesses, large or small, that are in compliance with other regulatory schemes requiring information security, such as the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act Security Rule, or the New York State Department of Financial Services' Cybersecurity Requirements for Financial Services Companies, are deemed compliant with the SHIELD Act.

Critically, the SHIELD Act specifically states that it does not confer a private right of action but rather provides for enforcement by the state's attorney general. The SHIELD Act's data security requirements take effect on March 21, 2020.

FREE CYBERSECURITY RISK ASSESSMENT SHOWS YOU HOW TO BE COMPLIANT WITH THE CURRENT LAWS AND AVOID POTENTIAL FINES

Most businesses lack the expertise or manpower to meet the robust requirements of the SHIELD Act. Instead, many are turning to cybersecurity experts like us to help them protect confidential information and achieve compliance.

Motiva remains vigilantly up to date on the constantly-changing threats created by cybercriminals. We have the expertise and tools to detect a wider range of attacks than in-house employees without the time or training to discover every possible breach.

Remember, it only takes one successful attack to cost companies large amounts of money and damage your credibility.

If you are concerned about employees and the dangers of cybercriminals gaining access to your network, then call us about how we can implement a managed security plan for your business.

At no cost or obligation, we'll conduct a FREE Cybersecurity Risk Assessment of your company's overall network health to review and validate as many as 10 different data-loss and security loopholes, including small-print weasel clauses used by all 3rd-party cloud vendors, giving them zero responsibility or liability for backing up and securing your data. We'll also look for common places where security and backup get overlooked, such as mobile devices, laptops, tablets and home PCs. At the end of this free audit, you'll know:

- Is your network really and truly secured against the most devious cybercriminals? And if not, what do you need to do (at a minimum) to protect yourself now?
- Is your data backup TRULY backing up ALL the important files and data you would never want to lose? We'll also reveal exactly how long it would take to restore your files (most people are shocked to learn it will take much longer than they anticipated).
- Are your employees freely using the Internet to access gambling sites and porn, to look for other jobs and waste time shopping, or to check personal e-mail and social media sites? You know some of this is going on right now, but do you know to what extent?
- Are you accidentally violating any PCI, HIPAA or other data-privacy laws? New laws are being put in place frequently and it's easy to violate one without even being aware; however, you'd still have to suffer the bad PR and fines.
- Is your firewall and antivirus configured properly and up-to-date?
- Are your employees storing confidential and important information on unprotected cloud apps like Dropbox that are OUTSIDE of your backup?

I know it's natural to want to think, "We've got it covered." Yet I can practically guarantee my team will find one or more ways your business is at serious risk for hacker attacks, data loss and extended downtime – I just see it all too often in the businesses we've audited over the years.

Even if you have a trusted IT person or company who put your current network in place, it never hurts to get a 3rd party to validate nothing was overlooked. I have no one to protect and no reason to conceal or gloss over anything we find. If you want the straight truth, I'll report it to you.

WHAT TO DO NOW: HOW TO REQUEST YOUR FREE ASSESSMENT

To request a Free Cloud Readiness Assessment, simply respond by:

1. Send me an email **walter@motiva.net**
2. Call us at **646-374-1820**

Because our Cybersecurity Risk Assessments take between five and seven hours to complete (with most of this "behind-the-scenes" diagnostics and research we conduct), I can only extend this offer to the first 20 people who respond. After that, we'll have to withdraw this offer or ask that you pay our customary consulting fee of $750 for this Assessment (sorry, no exceptions).

To respond, please call our office at 646-374-1820 and ask for me, Walter. I personally want to take your call to answer any questions about this letter, my company and how we might be able to help you, CEO to CEO. You can also e-mail me direct at walter@motiva.net.

Sincerely,

WALTER CONTRERAS
MOTIVA
Call Me Direct: 646-374-1820

WHAT DO OUR CLIENTS SAY ABOUT US?

★★★★★

"We never have to worry about our computer network. We have four law offices on Long Island that are in constant communication with each other and our clients. Motiva created our cutting-edge computer network and phone system, which has been a major factor in our rapid growth and our ability to keep costs down for our clients. Whenever we have issues with our computers or phones, we just send a message to Motiva, and our problems are solved."

David Sperling. President. Law Office Of David Sperling

★★★★★

"The convenience of a single source service between our phone system and our technology needs. Motiva's customer service team is very attentive, responds quickly and accurately. Having the continuity of service and depth of staff is very important. Motiva's staff maintains an excellent history of our inventory and always at the ready."

Alexander Badalamenti, President/CEO. BLD Architecture DPC

★★★★★

"I called Motiva 6 years ago, and I never looked back. They handle all of our Technology needs. Our delivery and order software has never run this smooth, and it's all thanks to Walter and his team. We open early in the AM, and there's always someone there to assist us if we have trouble. I don't know how they do it, but we have never been down. I highly recommend Motiva to any business."

Richard Bove, President Metal Masters Inc.

THE TOP 7 REASONS WHY YOU'LL WANT TO OUTSOURCE YOUR IT SUPPORT TO US:

✔ **We Have Deep Expertise in How Small to Medium Size Companies Operate their businesses.** We SPECIALIZE in IT services for small and mid-sized Companies in the New York area. We design, evaluate and justify technology solutions from a thorough understanding of the business benefit for your company.

✔ **We are the only IT Firm on New York that can can help you comply with the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) at no extra cost.** Our clients hire us when they want to make sure their IT systems are in compliance with New York State. Motiva's Compliance as a Service Plan is a "Done for you" compliance assurance. We hit every bullet point the law requires and monitors your systems for cyberattacks 24/7/365.

✔ **We Answer Our Phones LIVE.** You'll never call our office and be put into voice-mail Hell. Quality, professional support is always just a phone call away.

✔ **We do not OUTSOURCE anything.** We have 10 plus engineers on staff, so you don't have to wait on someone for support as you do with smaller firms. We also answer our phones live, with an average response time of 93 seconds or less. We also offer after-hours and weekend support at NO EXTRA COST. Because we understand the work week isn't 9 to 5.

✔ **We Guarantee A 93-Seconds or less Response Time On Emergency Tickets.** If you have an IT emergency that is preventing you from working, we guarantee to have a qualified tech working to resolve it in less than 3 minutes. For all other non-urgent problems, we guarantee a 30-minute-or-less response time. If we fail to meet that standard, that month's IT support is on us.

✔ **Cybersecurity is Paramount.** At Motiva we enforce Cybersecurity Best Practices to all our customers. We educate your team on cybersecurity threats and implement a robust cybersecurity monitoring and remediation system to keep your network safe and compliant with New York Laws.

✔ **Most Documented 5 Star GOOGLE Reviews.** We have the most documented 5 Star Google Reviews than any other IT Company in our area. Read hundreds of comments from New York Businesses we've helped.