Cyber Security Integration

PROBLEM: Cyber Risk, Vulnerabilities, Data Breach, Liability, Lawsuits, Legal Issues, etc. Small and medium sized businesses are the most vulnerable, and usually do not recover well or not at all after a major data breach. Suffering a breach is not a matter of if, but when.

If many of the homes in your neighborhood were broken into, would you ignore it, would you listen to someone who tells you it won't happen to you or your security is good enough?

If you are an integrator, are you concerned about the Internet of Things (IoT), IP cameras, DVR's, and your potential liability if one of your customers is breached via one of these devices you may have installed and/or monitor?

SOLUTION: Assess the state and quality of your security to determine whether there are any glaring vulnerabilities, the level of risk/liability to your company, and whether you may have already been breached.

At **CSI,** our goal is to help you lower the risk of a breach, reduce or eliminate the liability associated with a breach, and help you prepare to detect a breach and recover quickly. We do this by assessing your security, educating you on risks and vulnerabilities, as well as the risks to your customers, preparing a plan and assisting you in the implementation of that plan.

OFFERINGS

- **Free vulnerability scan**: the first step is to understand that despite yours and your IT peoples' best efforts, similar to most companies, you likely have many unknown vulnerabilities. Our scan will reveal these.

- **Overall Risk and Security Assessment**: (at a reduced price) This is a quick-look overview of the current state of your security. In addition to being aware of any vulnerabilities in your network you must understand the current state of your security and what risks exist. This knowledge will allow you to develop and implement a plan to mitigate the risks and move forward.

- **Full-Scope Assessment**: This assessment will include a full risk assessment, security audit, vulnerability test, penetration test, interviews and discussion of your risk as well as your customers and vendors since this will likely impact your company. At the completion of the of the full-scope assessment we will provide you with a comprehensive report of the findings and a detailed plan for improving your security, lowering risk and reducing or eliminating liability, and a plan for reacting to a breach.
- * This Assessment also meets the requirements of an annual assessment/audit required by some regulations and laws.

- **Policy Review and Drafting**: We will review any policies you have for completeness, and draft any that are missing to ensure your security program is well documented and to meet any compliance needs your company faces.

- **Cyber-Security Awareness Training**: We provide cyber security awareness training and programs to help you train the workforce and meet your annual requirements, compliance standards, and insurance requirements. We can provide annual or more frequent onsite training as well as develop a training program for you to utilize throughout the year to ensure all employees are frequently reminded of cyber issues, attacks, vulnerabilities and the standards and procedures you require be met.

- **Data Breach and Incident Response Investigation, Recovery and Resolution**: If you determine that you have suffered a breach we can provide all of the services necessary: investigations, forensics, messaging, legal support, and more, to ensure you recover quickly and minimize liability.

* We also provide attorney-client confidentiality when necessary.

The Consulting services provided by experts in risk management, security (cyber and physical), legal and regulatory compliance, technology, etc. The service is at a much reduced rate if a monthly fee based retainer is paid. In addition to the reduced rate for services when needed, the monthly fee includes an initial high level Risk Assessment and Executive Plan guidance and suggestions for fixing and improving.

Cyber-Security Liability and Risk Assessment Action Items
Action

- Conduct a Risk Assessment
- Prepare a Message in Anticipation of a Breach
- Draft/review/implement best practices, necessary policies and procedures
- Implement a comprehensive Cyber-Security Awareness Training Program

Benefits

- Lowers the risk of breach and reduces or eliminates potential liability associated with a breach
- Provides confidence to the leadership in their security program and ability to protect information
- Helps to Mitigate potential fines associated with non-compliance with (HIPAA/HITECH, SOX, GLBA, SEC and FTC Guidelines, PII, PCI, etc.), and avoid regulatory action by SEC, FTC, HHS, etc.

For a more complete understanding of the services and fees please contact us.

"Preparation is the key to lowering the risk of an attack and ensuring your Company can react quickly when a breach or incident is discovered!"

Custom Cyber Maturity Programs for Private Companies and Security Integrators:

We propose to provide the following: educational briefings to provide critical information related to threats and vulnerabilities for integrators and physical security systems and components, cyber security processes and techniques to better secure devices and networks, and high level plans and steps for moving forward toward more secure processes and infrastructure. We will also utilize this session to better understand your concerns and needs, answer questions related to risk management and security in the physical security and other spaces, and help you finalize the specifics of a plan for a comprehensive security plan based on your input and needs. This initial meeting will include insight, analysis and advice from our experts to educate, provide key steps to accomplish immediately, develop a comprehensive training plan and determine the best way forward.

In support of specific needs, Mr. Willson provides expert support in reviewing and drafting policy, educating the workforce on cyber security awareness and implementation, and planning for overall risk mitigation and security implementation.

Mr. Tendell will give an executive level presentation providing attendees a hacker's insight into the security vulnerabilities of physical security devices. He will share how physical security devices are normally hacked and the steps needed to make their next installation less of a target. Attendees of this session, "Hardware Hacking and How to Prevent It," will learn common attack scenarios for video, biometric, and access control devices and receive advice on prevention basics. The session will also address how to make security systems more secure by asking the right questions before and during an installation. Finally, Charles will provide an eye-opening demonstration of a typical system exploit.

Industry Segments and Cyber Security (Programs designed for Systems Integrators)

The Manufacturer will provide a speaker to discuss their products, vulnerabilities in the industry, and techniques for better securing devices and the information resident on or riding through these devices and networks. Some manufactures such as Axis are being proactive with their solutions and trying to educate Integrators on the proper techniques of installation and setup. Axis follows industry's best practices in managing and responding to security vulnerabilities with their products to minimize customers' exposure to cyber risks. Axis is dedicated to providing recommendations on how to reduce and eliminate risks relating to your Axis devices.

The Manufacturer will provide a speaker to address their products and better security for the industry. Today, more and more physical security systems are connected to IP Communication networks. This connection leaves the physical security systems Vulnerable to cyber-attacks, threatens national security and impacts public safety.

"Preparation is the key to lowering the risk of an attack and ensuring your Company can react quickly when a breach or incident is discovered!"

- Our experts are not your typical security experts but bring a much wider degree of expertise. For instance, experts agree that suffering a breach is not a matter of if, but when. For that reason, preparation is the key. Our legal-cyber expert, Dave Willson, can help you understand what is needed to minimize the risk of a breach, and eliminate or reduce the potential liability involved when a breach occurs, as well as help you recover quickly and protect your company and reputation while doing so. Our White Hat Hacker, Charles Tendell can investigate vulnerabilities and Larry Blumenfeld can advise on solutions as Physical Security relates to Cyber Security,

For a more complete understanding of the services and fees please contact us.

Phone – 336.549.6911 Email – larry@cybersecuritysecurityintegration.com

Management Team:

Larry Blumenfeld, BS Criminology, NCASLB, Cyber Security Integration (CSI) Former System Integrator and Founder of Access Control Consultants (ACC) for 23 years. (See separate Bio)

David Willson, JD, CISSP, Titan Info Security Group, Risk Management and Cyber Security Expert (See separate Bio)

Charles Tendell, CEH, CHFI, CISSP, Azorian Cyber Security, Cyber Security Expert and Ethical Hacker (See separate Bio)