TECH LOCK®
INCORPORATED

COMPLIANCE & DATA SECURITY

CHALLENGE QUESTIONS

PRESENTED BY: TODD LANGUSCH
TECH LOCK, INC.
1000 JOHN R RD, SUITE 201, TROY, MI 48083

Phone: 1.847.245.3727

E-mail: info@techlock.com | Website: http://www.techlockinc.com/

Legal Disclaimer

This information contained in this report is not intended to be legal advice and may not be used as legal advice. Legal advice must be tailored to the specific circumstances of each case. Every effort has been made to assure this information is up-to-date. It is not intended to be a full and exhaustive explanation of the law in any area, however, nor should it be used to replace the advice of your own legal counsel.

COMPLIANCE & DATA SECURITY

RISK ASSESSMENT

	How often does your company conduct a formal Risk Assessment, how is it performed and how are the results documented?
1	Is it sufficient in scope to identify the reasonably foreseeable threats from within and outside your operations that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer/consumer information systems, as well as the reasonably foreseeable threats due to the disposal of customer/consumer information?
2	Is it conducted at least annually?
3	Does it address reasonably foreseeable risks to customer/consumer information stored on systems owned or managed by service providers.
4	Does it address reasonably foreseeable risks to customer/consumer information disposed of by the service providers
5	Does it evaluate the potential damage from the identified threats?

REQUIREMENTS

GLBA Safeguards Rule 16 CFR Part 314

SECURITY AWARENESS

	How often does your company conduct employee security awareness training, how is it performed and how are the results documented?
1	Is it conducted at least annually?
2	Are staff trained to recognize and respond to schemes to commit fraud or identity theft, such as guarding against pretext calling?
3	Does your program provide staff members responsible for building or maintaining computer systems and networks with adequate training, including instruction about computer security?
4	Are staff properly trained in disposing customer information?
5	Does your program include signs, symbols, and stories?

REQUIREMENTS

GLBA Safeguards Rule 16 CFR Part 314

OVERSEEING SERVICE PROVIDERS

How does your company perform a due diligence on a service provider before signing a contract and how do you oversee and monitor those service providers on an ongoing basis?

1 Would you accept an SSAE 16 report from a Service Provider and call that service provider secure?

2 Does a PCI Scan certificate mean that service provider is PCI DSS compliant?

3 Do you have the service provider provide a data flow diagram so you know where your data goes, who touches it, how access is logged and what security controls are in place along the way?

4 Do you require your Service Providers to notify you in the event of a security incident or security breach? Do you require them to destroy your data and provide proof of destruction after the contract is over? Do you require your service provider to contractually be compliant with GLBA safeguards rule, PCI DSS, HIPAA, and other applicable laws and regulations?

5 Do you perform a reevaluation on all of your vendors at least annually?

ENCRYPTION

Protection methods such as encryption, truncation, masking, and hashing are critical components of consumer data protection. If unauthorized access to data occurs, with proper encryption and proper cryptographic keys are in place; the data should be unreadable

1 Do you have encryption at rest implemented for your collection system?

2 Do you encrypt all consumer data not located in your collection system? For example, call recordings stored on a file share or elsewhere? Do you have a listing of everywhere consumer data is stored – Sharepoint? Email? FTP server? FileShares? Laptops? Desktops?

3 Are all laptops encrypted?

4 Do you have more than two people that are encryption key custodians that do NOT have the entire key? Do you have a documented cryptographic key policy and key custodian agreement?

5 Do you change your cryptographic keys after a defined time period or when the integrity of the key has been weakened?

TRANSMISSION OF SENSITIVE OR NON-PUBLIC PERSONAL INFORMATION

Sensitive information must be encrypted during transmission over networks that are easily accessed by unauthorized individuals

1 Do you have wireless in your network? Is it outside of your corporate firewall and not on the internal network? Do you regularly scan for rogue wireless networks at least quarterly?

2 Do you have software or an appliance to scan outgoing emails to ensure no sensitive information leaves unencrypted?

3 Do you use strong cryptography when transmitting data over open public networks. For example SSL/TLS, IPSEC, SSH?

4 Do you disallow non-secure protocols at your firewall like FTP, TLS 1.0, SSH 1.0?

Sensitive information must be encrypted during transmission over networks that are easily accessed by unauthorized individuals

5 Do you have a DMZ at your firewall with email, ftp and other traffic stopped in the DMZ and no direct connections from the Internet to the backend internal network?

FIREWALL

Firewalls control traffic from trusted networks (your internal company network) to untrusted networks (Internet). All systems must be protected from unauthorized access from untrusted networks.

1 Is your firewall configured with specific configuration and hardening standards from available resources like www.cisecurity.org , www.nist.gov , or www.sans.org ?

2 Does your organization have documented any and all insecure protocols and business justification? Examples, but not limited to insecure services are FTP, Telnet, POP3, SNMP, IMAP, etc

3 Does your organization review firewall rules at least bi-annually and document this?

4 Does your firewall have egress filtering in place?

5 Does your firewall send its logs to a Syslog Server or SIEM device?

SYSTEM HARDENING

Unauthorized individuals often use default passwords, default accounts (administrator), systems with known weaknesses. To help organizations that are not security experts a number of security organizations have published configuration standards and guidelines to reduce your risk.

1 Does your company have documented configuration standards for all operating systems, databases, and enterprise applications?

2 Are all system default usernames disabled or renamed? Example Administrator in Windows, SA for SQL database, etc

3 Do IT staff or users with elevated privileged accounts have separate accounts for administration or do they use the same account for day to day tasks like web browsing or checking email as they do to administer the systems?

4 Does anyone in the company have administrative rights to their desktops or laptops? For example, can owners, VPs, or IT staff install programs on their own desktops or laptops with their normal user accounts?

5 Do all systems have file integrity monitoring software like OSSEC, Tripwire, Logrhythm or other FIM component to monitor critical files for changes?

REGULARLY MONITOR AND TEST

	Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. With vulnerabilities being discovered continually, system components should be tested frequently to ensure security controls continue to reflect a changing environment.
1	How do all of your servers, firewalls, switches, routers, collection system, and other enterprise applications log activity and how are those logs reviewed?
2	Is all access to all sensitive, non-public personal information logged? Collection system, call recordings, sensitive information stored on file shares or elsewhere?
3	Are ALL actions taken by any individual with root or administrative privileges logged and reviewed?
4	At a minimum, are the following audit trail entries recorded: user identification, type of event, date and time, success or failure, origination of event, and identity or name of affected data, system component, or resource?
5	The following are all different items and are all done: external scans on external devices and systems performed at least quarterly by a PCI ASV; quarterly internal scans done on internal systems and components performed by someone who does not patch the vulnerabilities; Penetration Tests (completely separate than vulnerability scans) performed by someone trained (CEH) using an approved methodology that includes both network layer and application-layer penetration tests performed at least annually and after any significant change?

STRONG ACCESS CONTROL MEASURES

	To ensure non-public personal information or sensitive data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know or job responsibilities
1	Do you have written policies that define access needs and privilege assignments for roles in your company?
2	Are access rights granted based on individual’s job classification and function?
3	Do your access control systems have a default “deny all” setting?
4	Does your company require documented approval by authorized parties specifying required privileges?
5	Does your company use least privileged policy and role based access (RBAC)?

GENERAL

	Questions
1	Does the executive team receive monthly security risk reports that outlines any security incident or intrusion attempts?
2	Do you do business outside of the United States? If no, then does your firewall or external router

	Questions
	block all traffic to/from outside the United States?
3	Do you have a Security Information Event Management Tool (SIEM) or some log monitoring tool? If no, how is it humanly possible to review all of the logs from all of the devices?
4	Can your IT Team tell you right now who is attacking you? With 2 out of 3 devices in the United Stated infected with malware, there is always someone knocking on your firewall or external router…do you know who?
5	Do you have an attorney that you send call recordings or account notes to? What due diligence was done on that attorney to ensure they are encrypting that data and have the proper security controls in place?

REMOTE ACCESS

	Questions
1	Does the company have two factor authentication in place…something that you know and something that you have physically for two factor remote authentication?
2	Is remote access performed over a VPN tunnel?
3	Is remote access performed using remote desktop or a terminal server?
4	Is Email allowed remotely on mobile devices?
5	Are Service Providers or other companies connected to your internal network through a VPN?