WorkSmarts Half-Day Seminar

Twists and Turns: Cybersecurity and Privacy Update

Shawn Tuma and Jeremy Rucker

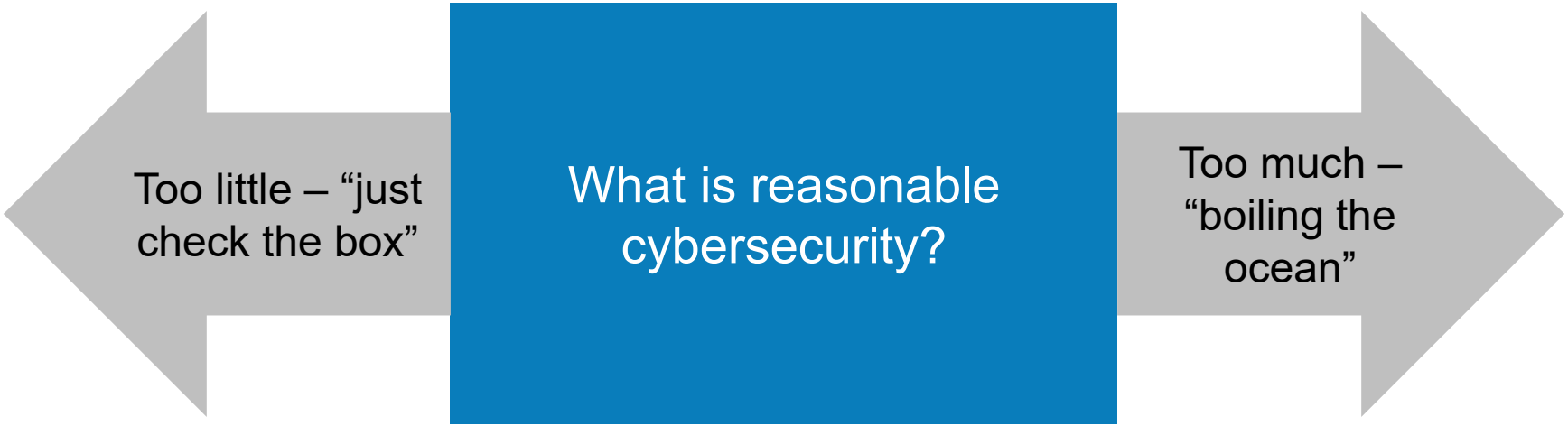
SpencerFane

Why a lawyer?

Cybersecurity is a legal issue

- Types of Laws
  - Security
  - Privacy
  - Unauthorized Access
- International Laws
  - GDPR
  - Privacy Shield
  - China's Cybersecurity Law
- Federal Laws and Regs
  - FTC, SEC, HIPAA, CISA
- State Laws
  - All 50 States
  - Privacy (50) + security (25+)
  - Comprehensive (CA, CO, CT, UT, VA)
- Contracts
  - Cyber Insurance
  - Industry Groups (*e.g.,* PCI & FINRA)
  - 3rd Party Bus. Assoc.
  - Privacy / Data Security / Cybersecurity Addendum

Cyber is an existential business risk.


Too little – “just check the box”
What is reasonable cybersecurity?
Too much – “boiling the ocean”

Reasonable cybersecurity is a process, not a definition

Cyber risk management program – assessment

The most essential step?

- How do you protect against what you don't know?
- How do you protect what you don't know you have?
- How do you comply with rules you don't know exist?
- Demonstrates real commitment to protect, not just "check the box compliance."
- No two companies are alike, neither are their risks, neither are their risk tolerances, neither are their mitigations.

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle." –*Sun Tzu*

What should your company's cyber risk management program look like?

Cyber risk management program requirements:

- Based on a risk assessment[1,2,3,4,5]
- Implemented and maintained (i.e., maturing)[1,2,3]
- Fully documented in writing for both content and implementation[1,2,3]
- Comprehensive[1,2,3,4,5]
- Contain administrative, technical, and physical safeguards[1,2,3]
- Reasonably designed to protect against risks to network and data[1,2,3,4,5]
- Identify and assess internal and external risks[2]
- Use defensive infrastructure and policies and procedures to protect network and data[1,2,3,4,5]
- Workforce training[2,3]
- Detect events[2]
- Respond to events to mitigate negative impact[2]
- Recover from events to restore normalcy2
- Regularly review network activity such as audit logs, access reports, incident tracking reports[3]
- Assign responsibility for security to an individual[3,5]
- Address third-party risk[2,3,5]
- Certify compliance by Chair of Board or Senior Officer or Chief Privacy Officer[2]

1. In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014)
2. NYDFS Cybersecurity Regulations Section 500.02
3. HIPAA Security Management Process,
4. SEC Statement and Guidance on 2/21/18
5. GDPR Art. 32

Employee Privacy Rights

- Based on state law
- State common law
  - Reasonable expectation of privacy
  - Intrusion on employee's reasonable expectation of privacy
  - Employer's legitimate business reason
- State statutes
- State constitutions

Employee Monitoring

- Based on common law invasion of privacy claims “intrusion upon seclusion”
  - Employer intentionally intruded upon employee’s solitude, seclusion, or private affairs
  - Intrusion would be highly offensive to a reasonable person
  - Employee suffered injury as a result of employer’s intrusion
- Did the employee have a reasonable expectation of privacy regarding emails and computer usage while on employer’s computer system.
  - Considerations for an expectation of privacy:
    - Did employer give notice to employees of computer policies and monitoring
    - Did employer allow use of computer systems for employee personal use
  - Employer’s justification for the monitoring
  - Reasonableness of employee’s expectation of privacy
- Employers should provide written notice and policies to employees regarding employer’s monitoring.
  - *Notice does not give employers free reign*

Artificial Intelligence

- AI in the employment setting: business + technology + privacy + legal
- Increased workplace monitoring
- Additional consent, notice, and explanation requirements for monitoring or interviewing
- White House Office of Science and Technology “Blueprint for an AI Bill of Rights” (Oct. 2022)
- Five principles help with the deployment of AI to protect individual rights:
  - Safe and Effective Systems: you should be protected from unsafe or ineffective systems
  - Algorithmic Discrimination Protections: you should not face discrimination by algorithms and systems should be used and designed in an equitable way
  - Data Privacy: you should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used
  - Notice and Explanation: you should know that an automated system is being used and understand how and why it contributes to outcomes that impact you
  - Human Alternatives, Consideration, and Fallback: you should be able to opt out, where appropriate, and have access to a person who can quickly consider and remedy problems you encounter

Artificial Intelligence

EEOC Guidance (May 2022)

- AI uses and potential violations of Americans with Disabilities Act
  - Employer fails to provide reasonable accommodation necessary for accurate algorithmic ratings
  - Tools that screen out disabled individuals
  - Tools that pose impermissible disability-related questions
- ADA prohibits employers with 15 or more employees from discriminating on the basis of disability.

Biometric Data

Laws governing biometric data

- Texas, Washington, Illinois
- Biometric data includes an individual's unique physical characteristics, such as fingerprints, retina or iris scans, or facial geometry.
- Uses
  - Security features
  - Track employee time
- Employee must give informed consent.
- Duty of employer to exercise reasonable care in the storage and transmission of biometric data

Data Breaches

Employers must protect employee data from unauthorized disclosure.

- Breach notification laws (all 50 states)
- Employee data may be protected
- Disclosure requirements:
  - Affected individuals
  - Regulators (state and/or federal)
  - Media outlets
  - Credit bureaus
- Protected data varies by state; generally, includes names in combination with SSNs, driver's license number or other government-issued ID; financial information; (others)

State Comprehensive Privacy Laws

	Right of Access	Right of Rectification	Right of Deletion	Right to restrict processing (targeting/advertising)	Right of Portability	Right to opt out of sales	Right against automated decision making	Private Right of Action	Applies to HR data
California (Jan 1,2023)	X	X	X	X*	X	X	X	X*	X
Colorado (July 1, 2023)	X	X	X	X	X	X	X		
Connecticut (July 1, 2023)	X	X	X	X	X	X	X		
Virginia (Jan 1, 2023)	X	X	X	X	X	X	X		
Utah (Dec 31, 2023)	X		X	X	X	X			

State Comprehensive Privacy Laws

Most state comprehensive privacy laws exclude HR data

Majority of compliance obligations rest with staff

- Ensure consumer requests are properly addressed
- Workforce training requirements
- Incident response teams
- Development and implementation of policies (e.g., data retention policies)
- Vendor management team ensuring contracts contain required terms
- Implementation of security practices and procedures

It’s all about the data

- The laws focus on the data – usually “personal data” – even the “cybersecurity” laws.
- “[H]elps businesses protect their information and protect themselves from their information.” Data = risk.
- How do you protect what you do not know you have, where it is stored, how it is used?
- Policies, procedures, and training are the foundation for protecting data.
- Good focus for due diligence on cyber and privacy risk.

Data governance

- Data governance is the process of managing the availability, usability, integrity and security of the data in enterprise systems, based on internal data standards and policies that also control data usage.
- Minimum “must have” policies and procedures:
  - Data Map
  - Limited collection based on need and use
  - Segregation of data with limited privilege access
    - Manage storage and enforce controls
  - Effective and utilized Data Retention/Destruction Policy
    - Include email accounts
    - Archive and encrypt or securely destroy (and document the process!)
- Workforce training on policies, procedures, and “the why” for each.

Acceptable use policy

- Every company must have an “acceptable use” policy that covers both the company (1) computer system and (2) data.
- Your company is responsible for how its computer system is use and how its data is used and protected – if an employee takes that data for improper purposes, it is your company’s data breach.
- This policy is where you set expectations and set limitations.
- Use should be reasonably limited to “for business purposes” for using the computer system and should strictly limit access, use, and obtaining of data “for business purposes only.”
- Should spell out requirements and limitations for using both computer system and data.
- Should make clear that the company has the right to and will monitor usage of both and there is no expectation of privacy.
- Foundation for using unauthorized access laws for “insider misuse,” which is very common.

HR data is very risky

- HR data is often some of the most valuable and sensitive in the company.
  - SSN, DOB, salary, banking/retirement accts, tax, employee files/reviews.
  - Current, former, prospective employees – sometimes dating back decades.
- Employee data compromise is a data breach, just like customer data.
  - B2B companies – employee data is often the riskiest data.
  - Disgruntled former employees most likely to sue and assemble class.
- Threat actors know this and specifically attack HR data in cyber-attacks.
  - Email phishing schemes for W-2 information especially prevalent in Q1.
- Need good data governance, internal controls, workforce training.
- Same risks and recommendations apply for Accounting Department.

BEC attacks are costly

Messages

From <app_ipods@lycos.com>

To

Subject Re: Aging Report

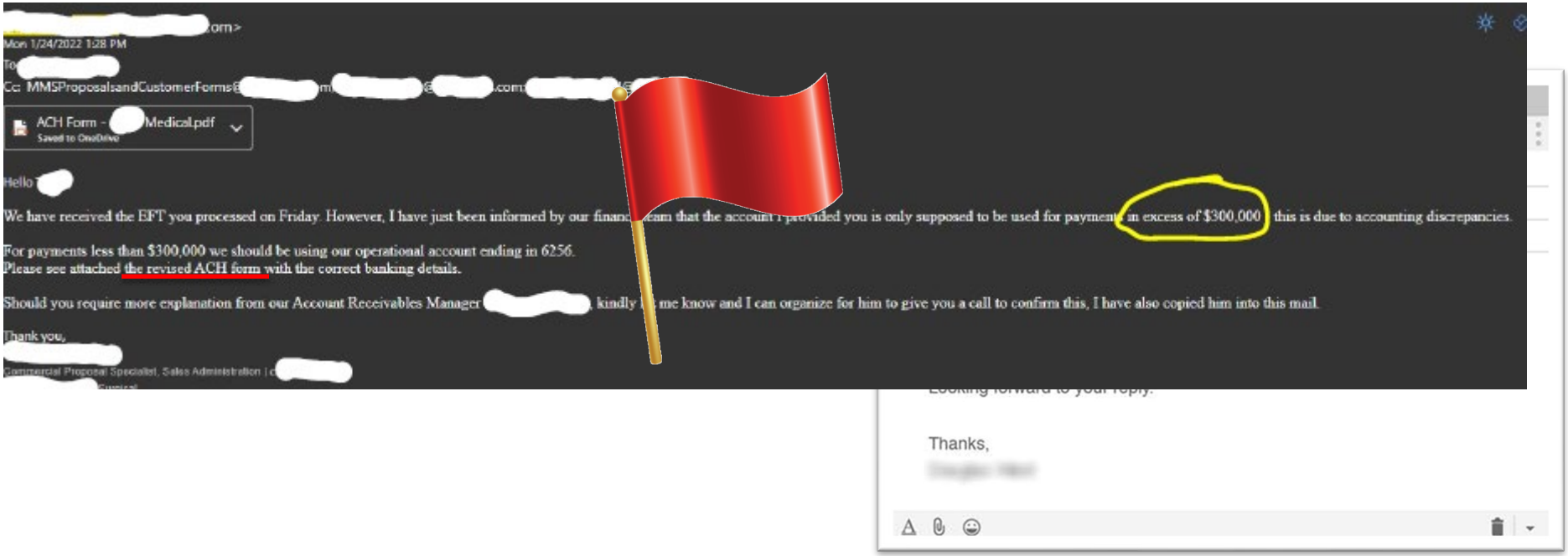
Hi

I need you to email me the aging report from A/R, and also include customer payable contact email on this report.

Looking forward to your reply.

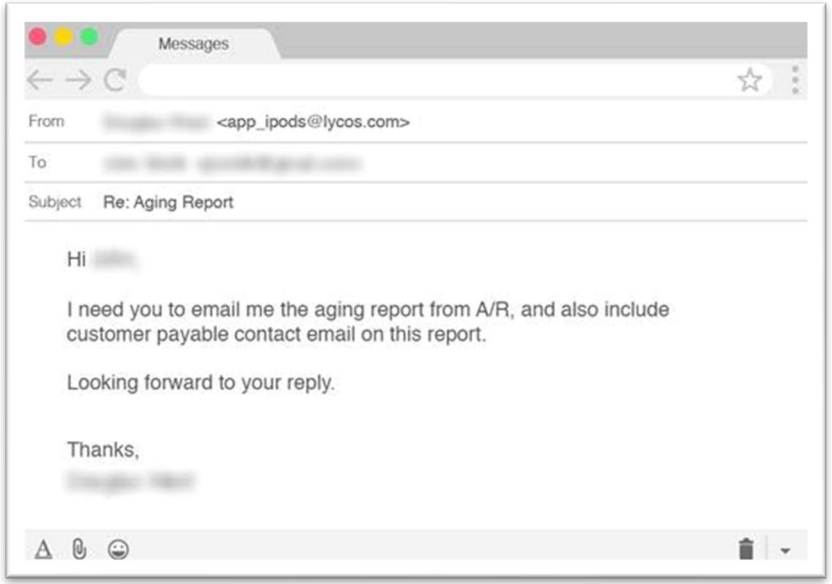
Thanks,

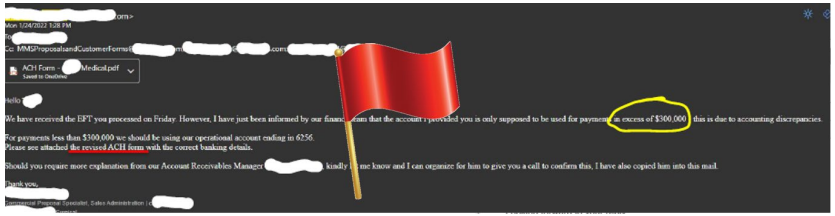
BEC attacks are costly



BEC attacks are costly

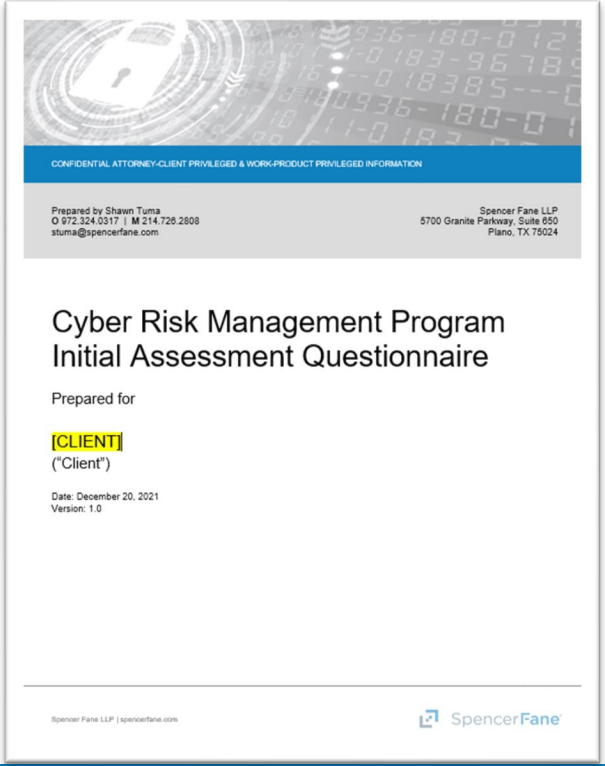
- Business Email Compromise (BEC) attacks are often the simplest and costliest.
- Results from 2 failures:
  - Email account “hack”, because no 2FA
  - Lack of “internal controls” in company
- What internal controls are needed?
- Key issue for supply chain risk.
- Cyber insurance understanding and interrelationship is critical.





Handout Materials & Information

Initial Assessment Questionnaire



CONFIDENTIAL ATTORNEY-CLIENT PRIVILEGED & WORK-PRODUCT PRIVILEGED INFORMATION

Prepared by Shawn Tuma
O 972.324.0317 | M 214.726.2808
stuma@spencerfane.com

Spencer Fane LLP
5700 Granite Parkway, Suite 650
Plano, TX 75024

Cyber Risk Management Program
Initial Assessment Questionnaire

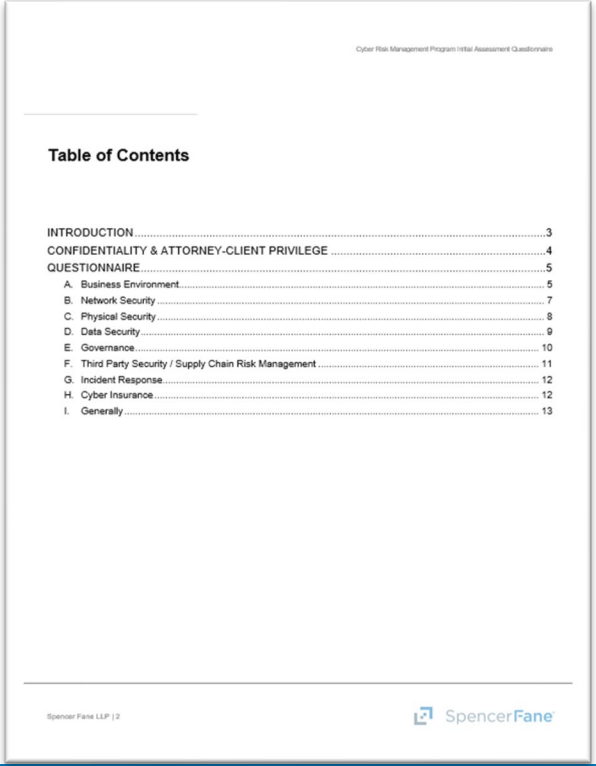
Prepared for

[CLIENT]
("Client")

Date: December 20, 2021
Version: 1.0

Spencer Fane LLP | spencerfane.com

SpencerFane



Cyber Risk Management Program Initial Assessment Questionnaire

Table of Contents

INTRODUCTION 3
CONFIDENTIALITY & ATTORNEY-CLIENT PRIVILEGE 4
QUESTIONNAIRE 5
A. Business Environment 5
B. Network Security 7
C. Physical Security 8
D. Data Security 9
E. Governance 10
F. Third Party Security / Supply Chain Risk Management 11
G. Incident Response 12
H. Cyber Insurance 12
I. Generally 13

Spencer Fane LLP | 2

SpencerFane

Strategic Plan & Timeline

Phase I Plan & Timeline

Action Items for Phase I Plan

CONFIDENTIAL ATTORNEY/CLIENT PRIVILEGED COMMUNICATION

An analysis of the Initial Assessment Questionnaire and the notes from our meeting and have the following ac
items that we need to complete for Phase 1 of this process, listed below:

Action Items	Status	Anticipate Completio
1. Work with Spencer Fane (cybersecurity attorney) on Phase I		
1.1. Retain Cyber [redacted]	Completed	
1.2. Complete Cyber Risk Initial Assessment Questionnaire	Completed	
1.3. Work through results of Questionnaire, discuss goals, process and planning	Completed	
1.4. Prepare and implement Computer System Acceptable Use Policy (2 versions: managerial level and basic level for entry level workers)	Completed	
1.5. Prepare and implement additional information technology, security, and compliance and oversight policies	Deferred	
1.6. Prepare and conduct managerial level workforce training on basic policies and procedures, to be recorded for future worker onboarding	Deferred	
1.7. Implementation of the following recommendations:		
1.7.1. Backup redundancy and offline storage	Completed	
1.7.2. Multifactor authentication	Completed	
1.7.3. Encryption of laptops	Deferred	
1.7.4. Phishing training and testing (+ adding "EXTERNAL" marking to emails)	Completed	
1.7.5. Logging (increased level and retention)	Completed	
1.7.6. Physical security of technological devices	Completed	
1.7.7. [redacted] – diligence review of security procedures	Completed	
1.7.8. [redacted] – diligence review of contracts	Deferred	

Spencer Fane LLP | spencerfane.com

SpencerFan

Phase I Strategic Plan & Timeline

Action Items for Phase I Strategic Plan

CONFIDENTIAL ATTORNEY/CLIENT PRIVILEGED COMMUNICATION

An analysis of the Initial Assessment Questionnaire and the notes from our meeting and have the following
items that we need to complete for Phase 1 of this process, listed below:

Action Items	Status	Anticip Compl
1. Work with Spencer Fane (cybersecurity counsel) on Phase I		
1.1. Complete Cyber Risk Initial Assessment Questionnaire		
1.2. Work through results of Questionnaire, discuss goals, process and planning		
1.3. Determine applicable legal and regulatory jurisdictions		
1.3.1. Examine and confirm NYDFS applicability		
1.3.2. Confirm NYDFS meets "industry recognized framework" requirements of Colorado, Connecticut, Ohio, and similar state laws		
1.4. Retain dedicated cybersecurity provider (Cybersecurity Firm) to obtain penetration testing / cybersecurity assessment		
1.5. Policies & Procedures		
1.5.1. Handbook Policies		
1.5.1.1. Remove those listed below as standalone and refer to them		
1.5.1.2. Social Media – review current NLRA guidance		
1.5.2. Prepare and implement the following policies:		
1.5.2.1. Computer System Acceptable Use Policy		
1.5.2.2. Bring Your Own Device		
1.5.2.3. Privacy Policy		
1.5.2.4. Privacy Notice (website – analysis of need) Analysis of California requirement for data removal button		
1.5.2.5. Data Classification		
1.5.2.6. Document Retention (see suggestions in draft with data		

Spencer Fane LLP | spencerfane.com

SpencerF

Strategic Plan & Timeline

Action Items for Strategic Plan

CONFIDENTIAL ATTORNEY/CLIENT PRIVILEGED COMMUNICATION

Based on analysis of the Initial Assessment Questionnaire, the risk assessment process, and information from subsequent meetings, the following action items are current recommendations to consider for future phases of this process to continue maturing cyber resilience, preparation, and readiness:

Action Items	Status	Anticipated Completion
1. Work with Spencer Fane (cybersecurity counsel) on Risk Assessment and Developing Strategic Plan & Timeline	In Progress	10/8/21
1.1. Complete Cyber Risk Initial Assessment Questionnaire	Complete	9/9/21
1.2. Work on Risk Assessment through Questionnaire responses, meetings with client, collection of information, discussion of goals, overall process, and planning	Complete	9/27/21
1.3. Analysis of information, prioritization of objectives, and development of overall Strategic Plan and Timeline	Complete	10/12/21
2. Identify Critical Areas of Risk	Complete	10/12/21
2.1. Crown Jewels	Complete	10/12/21
2.1.1. [redacted] platform	Complete	10/12/21
3. Incident Response Preparation		**Phase 2**
3.1. Develop Security Incident Response Team (SIRT) (Internal & External)	In progress	
3.1.1. Interview and engagement of key vendors		Phase 2
3.1.2. Confirm approval of External SIRT under cyber insurance coverage (when obtained)		Phase 2
3.2. Internal SIRT conference and whiteboard key risks and vendors for incident response		Phase 2
3.3. Establish federal law enforcement liaisons	Complete	
3.4. Prepare Incident Response Quick Reaction Plan *note: Complete IRP will be in Phase 2	Complete (but will	

Spencer Fane LLP | spencerfane.com

SpencerFane

Cyber Incident Quick Reaction Sheet

Cyber Incident Quick Reaction Sheet

SpencerFane

Title	Company	Contact Information	Backup Contact Information
Incident Response Team	[Internal -- CISO / CIO / CTO / ...]		
	[Internal -- Security]		
	[Internal -- IT]		
	[Internal -- Privacy]		
	[Internal -- GC]		
	[Internal -- Operations]		
	[Internal -- Communications]		
	[Internal -- CFO]		
	[Internal -- HR Member]		
	[External - IT MSP Provider]		
	External -- MSSP / SOC Provider		
	[External -- Cybersecurity]		
	[External -- Breach Counsel] Spencer Fane, LLP Shawn Tuma	d 972.324.0317 m 214.726.2808 stuma@spencerfane.com cyber@spencerfane.com	Jeremy Rucker d 214.459.5880 m 817.821.5002 jrucker@spencerfane.com
IT MSP Provider			
MSSP / SOC Provider			
Cloud Services Provider			
Breach Counsel	Spencer Fane LLP	Shawn Tuma d 972.324.0317 m 214.726.2808 stuma@spencerfane.com cyber@spencerfane.com	Jeremy Rucker d 214.459.5880 m 817.821.5002 jrucker@spencerfane.com
Cyber Insurance Carrier, Policy # and Policy location			
Cyber Insurance Broker			
Cybersecurity / Cyber Forensics Vendor			
Decryption/Negotiation Vendor			
FBI Contact		Richard Murray d 972.559.5231 m 505.948.8463 rmurray@fbi.gov FBI Online Reporting: www.ic3.gov	Brett Leatherman d 972-559-5132 m 248-207-6616 bleatherman@fbi.gov
Human Resources Personnel			
Vice President of Operations			
Public Relations Team			
Payment Card Processor & Processor Agreement location			
PFI Investigator			
Breach Notification Vendor	IDX	Todd Hindman m 512.712.2270 todd.hindman@idx.us	
Key Notes & Information			

Spencer Fane LLP | spencerfane.com

Tips to prepare for resilience

Questions to ask your breach coach

1. Have you collectively brainstormed to think about your greatest cyber risks?
2. Do you have an Incident Response Plan (IRP)? Cyber Incident Quick Reaction Sheet?
3. Do you know when to activate the IRP?
4. Does each member of the Security Incident Response Team (SIRT) understand his or her role and responsibility under the IRP?
5. Do you have redundancies for those roles and responsibilities?
6. Do you know who is the “head coach” and, what if that person is unavailable?
7. Do you know what external parties are needed under the IRP?
8. Do you have easy access to all internal and external parties’ contact information, with redundancies, including personal cell numbers?
9. Do you have relationships already established with those third parties?
10. Do you have those third parties pre-approved under your cyber insurance policy?
11. Do you have your insurance policy, policy number, and claims contact information handy?
12. How will you access all of this information if your network is down?
13. Have you practiced a mock scenario to test your preparedness? What about if your “head coach” is unavailable?

Tips to better protect your company

1. Perform a risk analysis to better understand your organization's greatest risks – you cannot mitigate what you do not know exists.
2. Backup your data, system images, and configurations, regularly test them, and keep at least one copy of the backups offline. Consider the "3-2-1 backup rule."
3. Encrypt all sensitive data to ensure that if it is stolen its confidentiality is not compromised.
4. Update and patch your systems promptly, especially external-facing systems. Configure automatic updates on workstations and laptops where feasible.
5. Require multifactor authentication (MFA) for every login for something important, especially external-facing systems and services. MFA is using two steps to login instead of just one.
6. Require cybersecurity and phishing training and exercises for all members of your organization, especially senior leadership.
7. De-escalate privilege to the minimum necessary on user accounts, especially for high value target users such as executives, accounting, human resources, and for vendor access.

Tips to better protect your company (pt. 2)

8. Use a reputable firewall that is configured to block access to known malicious IP addresses.
9. Use a reputable endpoint detection and response (EDR) solution.
10. Identify external-facing systems by looking up IP addresses and DNS subdomains for your organization.
11. Block public access to the services Remote Desktop Protocol (RDP), Secure Shell (SSH), Telnet, and File Transfer Protocol (FTP).
12. Perform vulnerability scans against external-facing systems.
13. Have a security team and check their work.
14. Have an incident response plan and business continuity plan and regularly exercise both.
15. Segment your networks.
16. Choose third-party service providers that are dependable and secure.

Thank You

Shawn Tuma

Partner | Plano, TX

972.324.0317 | stuma@spencerfane.com

Jeremy Rucker

Associate | Plano, TX

214.459.5880 | jrucker@spencerfane.com