

MASTER CLASS: Data Protection and Cybersecurity

Shawn E. Tuma
Co-Chair, Data Privacy & Cybersecurity
Spencer Fane LLP
www.spencerfane.com
stuma@spencerfane.com
o: 972.324.0317
m: 214.726.2808



Why a lawyer?

Neiman Marcus

SuperValu
Real

SONY

Michaels

STAPLES

AdultF

EQUIFAX

ASHLEY
MADISON®
Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See Your Matches»

Over 22,995,000 anonymous members!



K

DQ

NEW YORK
STATE OF
OPPORTUNITY

Y
YAHOO!

Capital One

Albertsons



P.F. CHANG'S
CHINA BISTRO

SALLY
BEAUTY SUPPLY

Health Systems

ups

sourcebooks

Affinity

BRAZZERS

JPMorganChase

bebe

SONIC

WHITE LODGING

Credit: NASA's Goddard Space Flight Center / Jeremy Schnittman

Cybersecurity is a legal issue

- Types
 - Security
 - Privacy
 - Unauthorized Access
- International Laws
 - GDPR
 - Privacy Shield
 - China's Cybersecurity Law
- Federal Laws and Regs
 - FTC, SEC, HIPAA
- State Laws
 - All 50 States
 - Privacy (50) + security (25+)
 - CCPA, NYDFS, Colo FinServ
- Industry Groups
 - PCI
 - FINRA
- Contracts
 - 3rd Party Bus. Assoc.
 - Privacy / Data Security / Cybersecurity Addendum

**OH, YOU STILL THINK YOUR
DATA IS NOT VALUABLE?**

**TELL ME MORE ABOUT THIS
RANSOMWARE**



Albany Mayor Kathy Sheehan ✓
@MayorSheehan

The City of Albany has experienced a ransomware cyber attack. We are currently determining the extent of the compromise. We are committed to keeping you informed and will provide updates as they become available.

12:44 PM · Mar 30, 2019 · Twitter for iPhone

HAPPENING NOW

NEWS10.COM

CYBER ATTACK HITS CITY OF ALBANY

**THINK YOUR
VALUABLE?**

**TELL ME MORE ABOUT THIS
RANSOMWARE**



Texas Department of Information Resources ✓
@TexasDIR

We are leading the response to a ransomware attack on at least 20 Texas local government entities. For more information, including #ransomware facts and cybersecurity tips see our attached guides and visit our website at dir.texas.gov/View-About-DIR...

STOP | THINK | CONNECT
RANSOMWARE FACTS & TIPS

As technology evolves, the prevalence of ransomware attacks is growing among businesses and consumers alike. It's important for digital citizens to be vigilant about basic digital hygiene in an increasingly connected world.

WHAT IS RANSOMWARE?
Ransomware is a type of malware that accesses a victim's files, locks and encrypts them and then demands the victim to pay a ransom to get them back. Cybercriminals use these attacks to try to get users to click on attachments or links that appear legitimate but actually contain malicious code. Ransomware is like the "digital kidnapping" of valuable data - from personal photos and memories to client information, financial records and intellectual property. Any individual or organization could be a potential ransomware target.

FIVE EVERY DAY STEPS TOWARDS ONLINE SAFETY

Cybersecurity is present in every aspect of our lives, whether it be at home, work, school, or on the go. Regardless of one's technical ability or background, there are simple steps everyone can take to stay safe online.

SIMPLE TIPS

Protect yourself online and help to make the internet safer and more secure by following these simple tips from the Stop Think Connect™ campaign:

- **Enable stronger authentication.** Always enable stronger authentication for an extra layer of security beyond the password that is available on most major email, social media and financial accounts. Stronger authentication (e.g., multi-factor authentication that can use a one-time code texted to a mobile device) helps verify that a user has authorized access to an online account. For more information about authentication, visit the new Lock Down Your Login Campaign at lockdownyourlogin.com.

Estimated Ransomware Costs – Texas 2019

Category	Estimated Cost
County	\$3,250,000
City	\$2,340,000
Education	\$1,800,000
Unreported	\$5,000,000

2:53 PM · Aug 17, 2019 · Twitter Web App

54 Retweets 45 Likes



Zack Whittaker ✓
@zackwhittaker

Following

The source said it took days for Arizona Beverages to get an incident response team in, leaving some to process customer order manually. The company's response to the ransomware attack was described as a "shitshow."

More: tcrn.ch/2TTqqTW

The ransomware also infected the company's Windows-powered Exchange server, knocking out email across the entire company. Although its Unix systems were unaffected, the ransomware outbreak left the company without any computers able to process customer orders for almost a week. Staff began processing orders manually several days into the outage.

"We were losing millions of dollars a day in sales," the source said. "It was a complete shitshow."

1:30 PM - 2 Apr 2019

31 Retweets 73 Likes



7



31



73





Texas D
@Texas

The C
attack
comp
inform
availa

We are le
at least
inform
cyber
web

12:44 PM

NEWS10.com

Zack Whittaker

@zackwhittaker

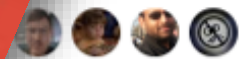
Following

...ce said it took days for Arizona
...get an incident response
...to process

The company's
...ck was

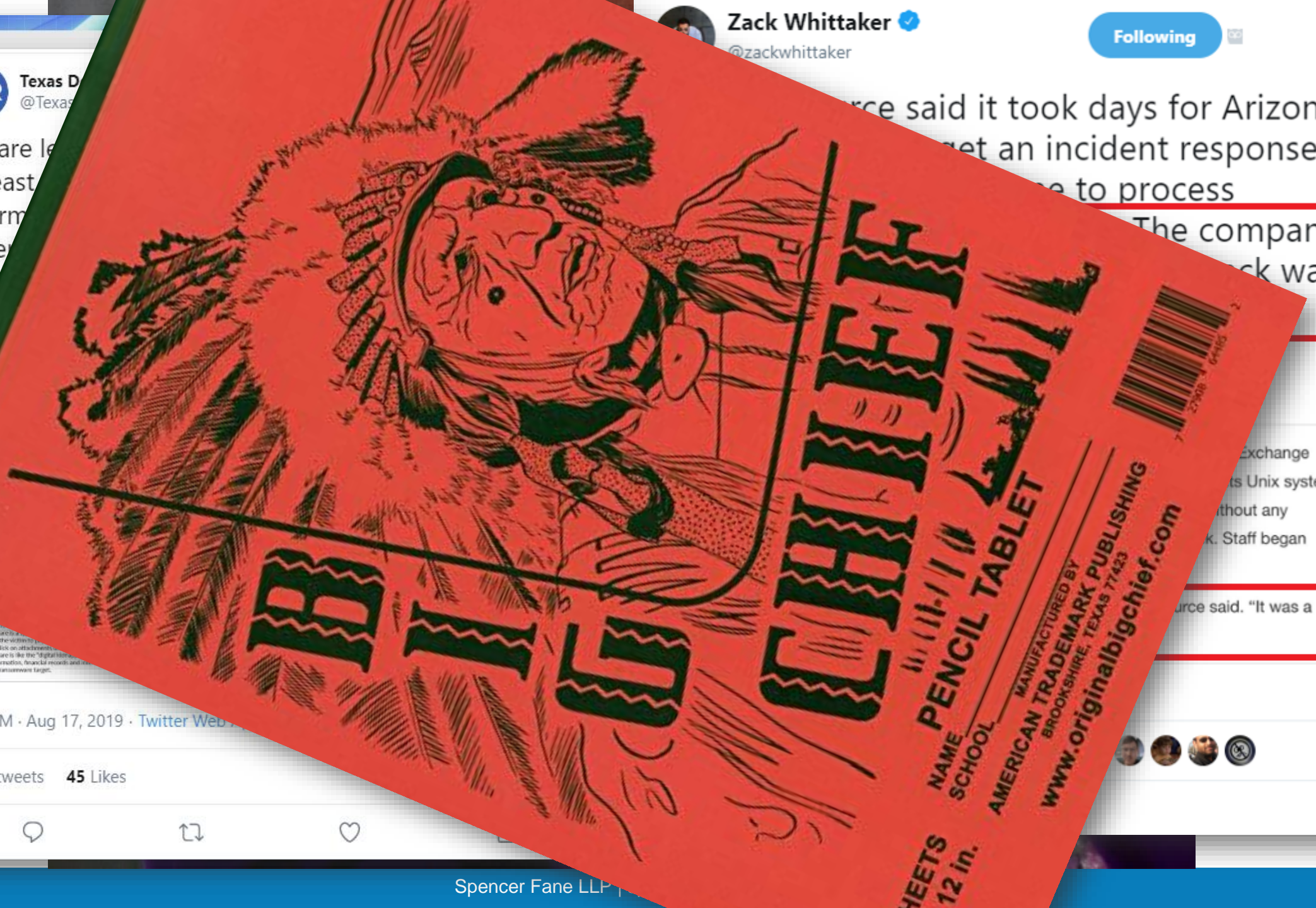
Exchange
...ts Unix systems
...without any
...k. Staff began

...source said. "It was a



2:53 PM · Aug 17, 2019 · Twitter Web

54 Retweets 45 Likes



Recap: Cybersecurity is no longer just an IT issue – it is an overall business risk issue – indeed, the ONE risk...

What we know



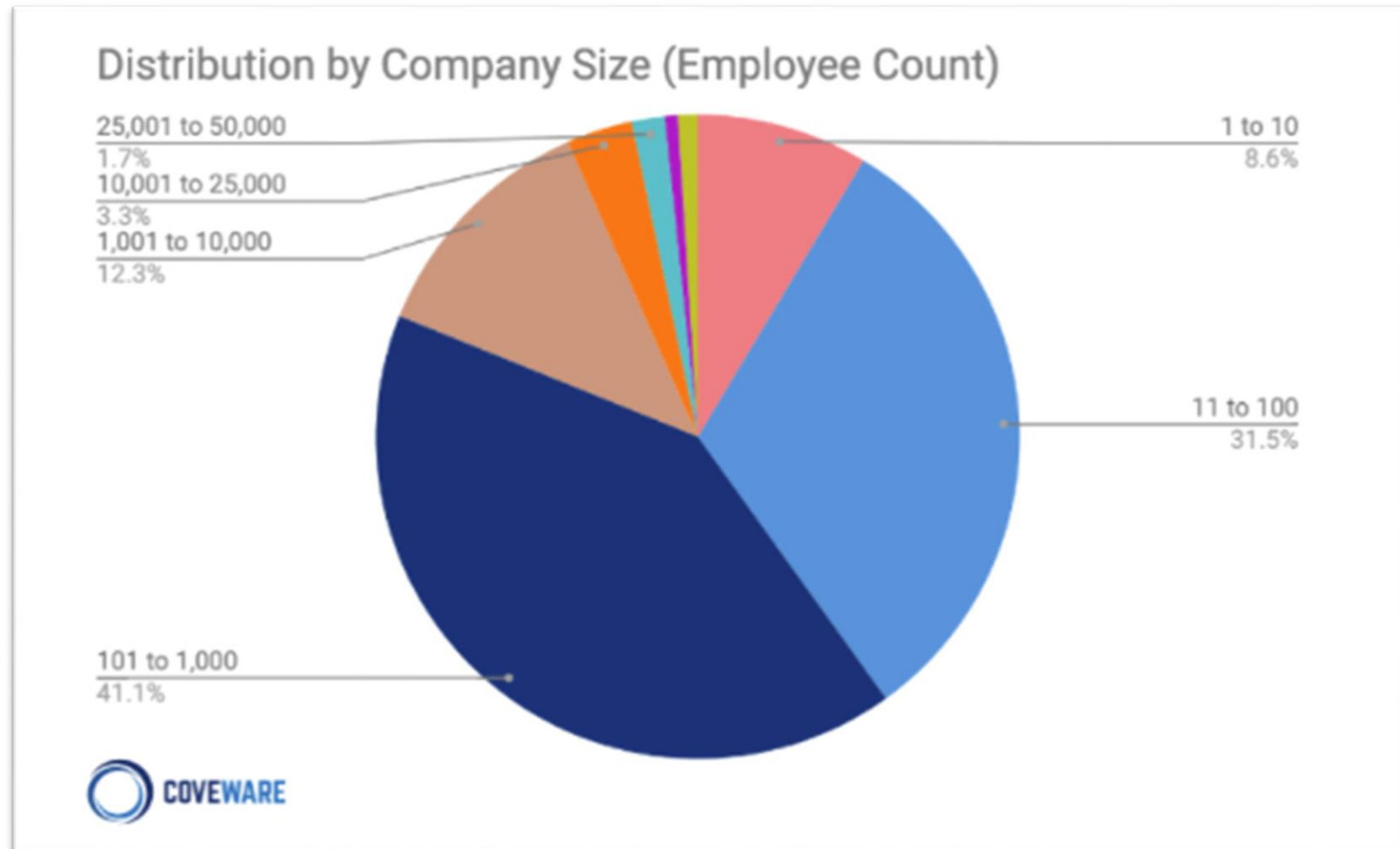
SpencerFane

What is ransomware?

- Ransomware is malicious software, or malware, that threat actors use to encrypt your data and deny you access to it until a ransom is paid.
- Nobody cares how intrinsically valuable your data is.
- You need it. The hackers know it. You will pay to get it.
- Also – exfiltration + publication is the recent trend (+ calling, ++ reporting crimes).

Who is at risk from an attack?

- Every type of organization with a computer connected to the internet is at risk.
- Every single one.
- Scanning tools.
- Yes, yours also!



What is the impact if you get hit?

- Your computer systems are shut down.
- You have no access to your data.
- Any operations requiring either computers or data are now shut down.

Downtime from a Ransomware Attack is still the most Dangerous Complication

Average Days of Downtime

19

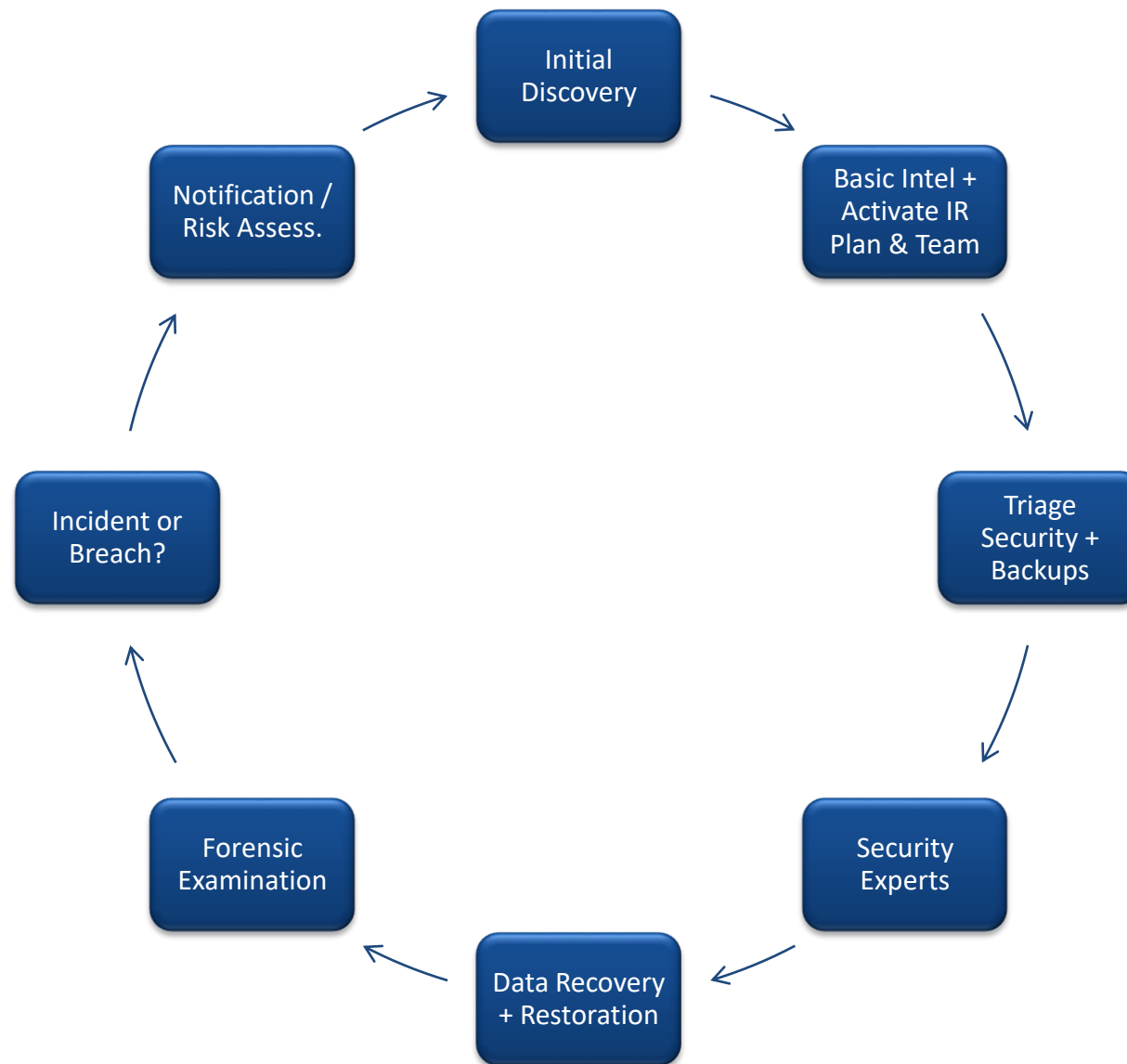
+19% from Q2 2020

How much are companies paying?

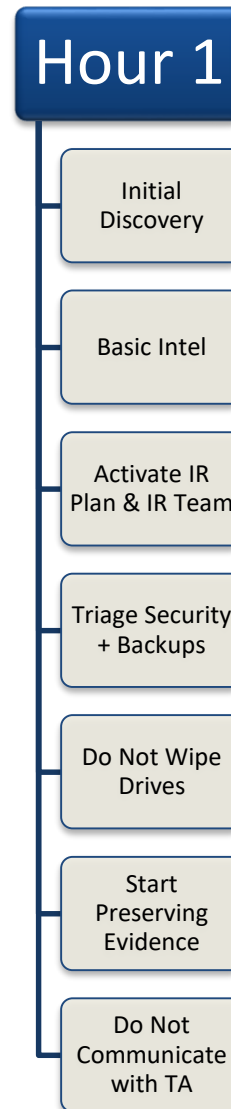


Recap: Every organization has substantial cyber risk

Ransomware response & recovery lifecycle



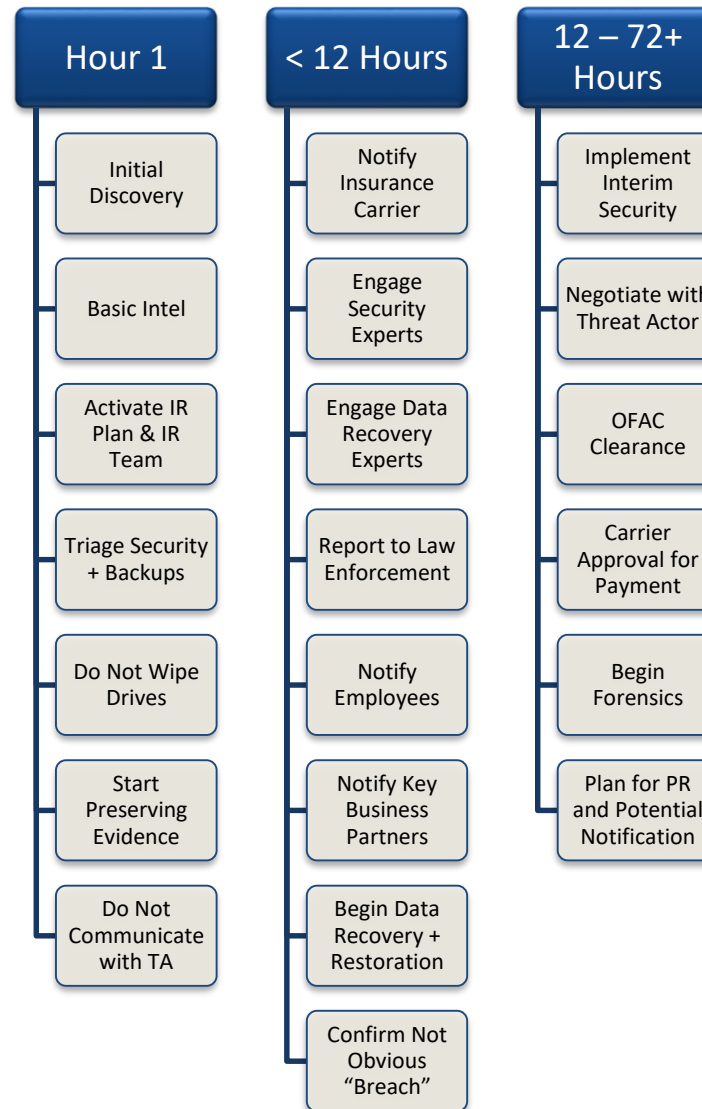
Ransomware response & recovery timeline



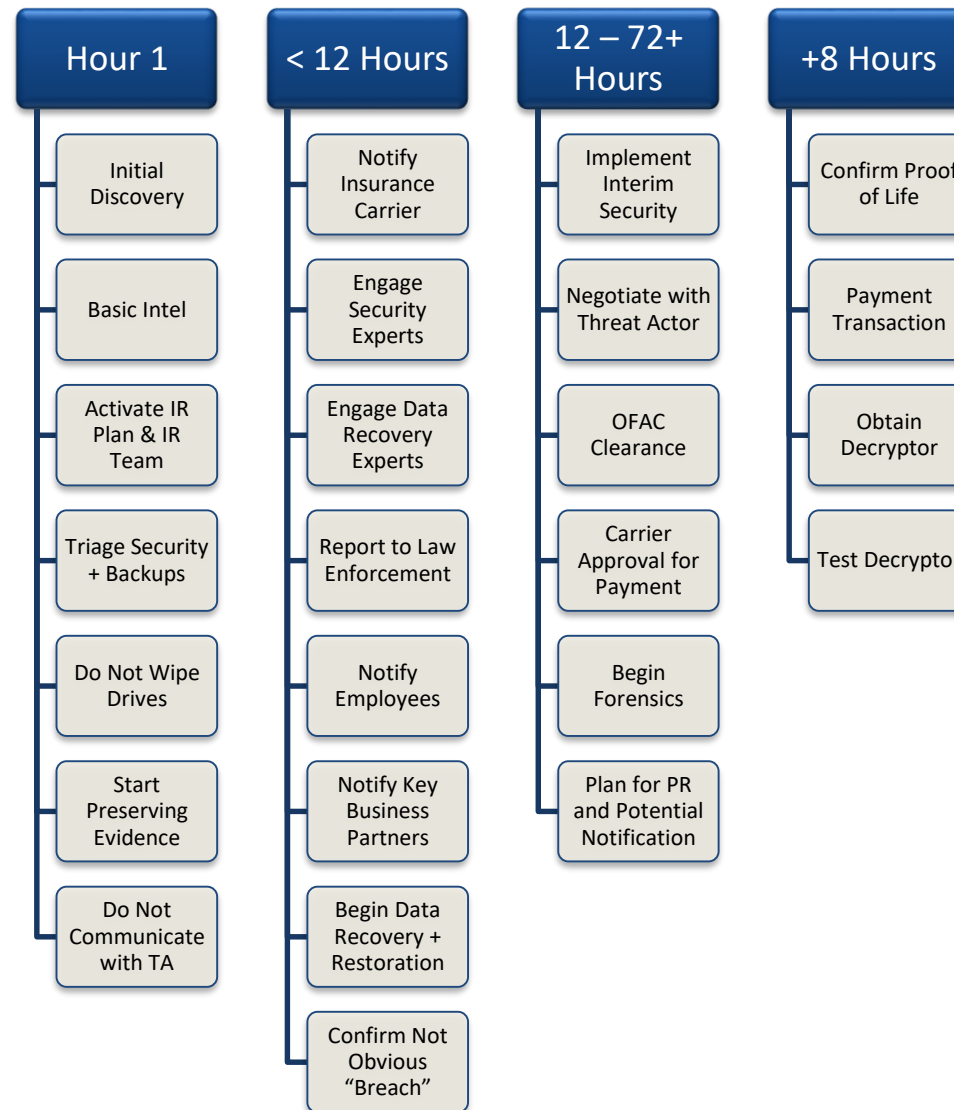
Ransomware response & recovery timeline



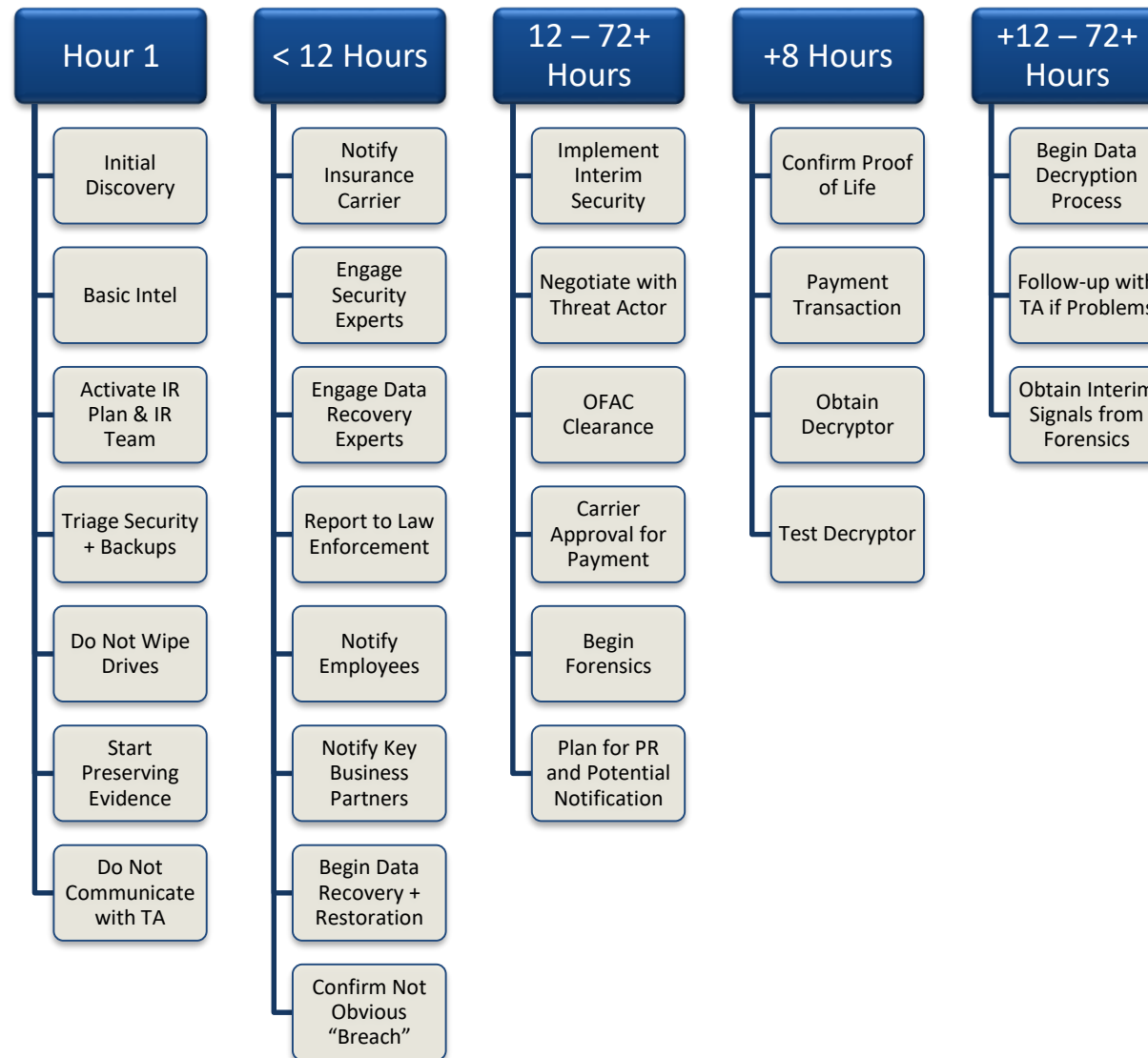
Ransomware response & recovery timeline



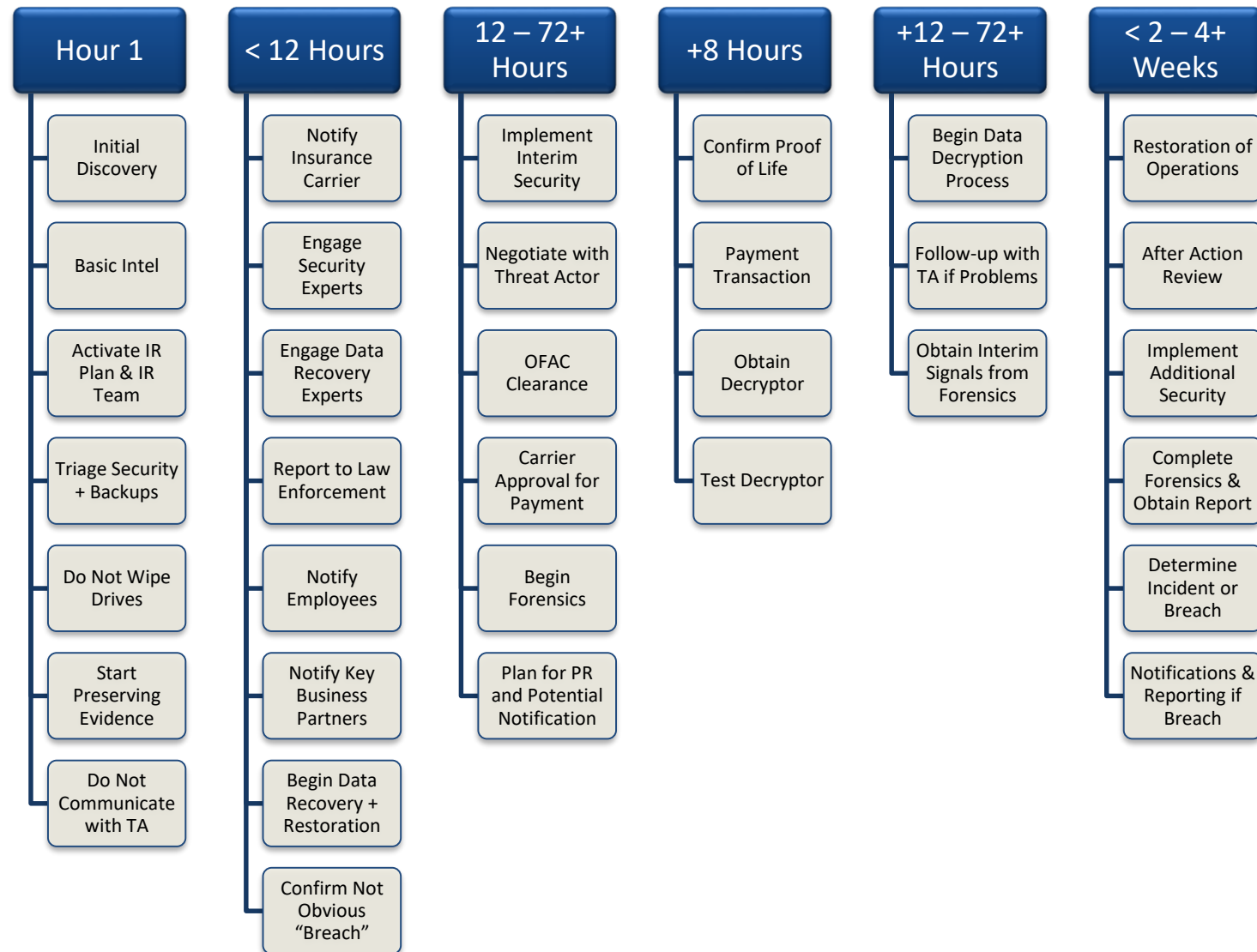
Ransomware response & recovery timeline



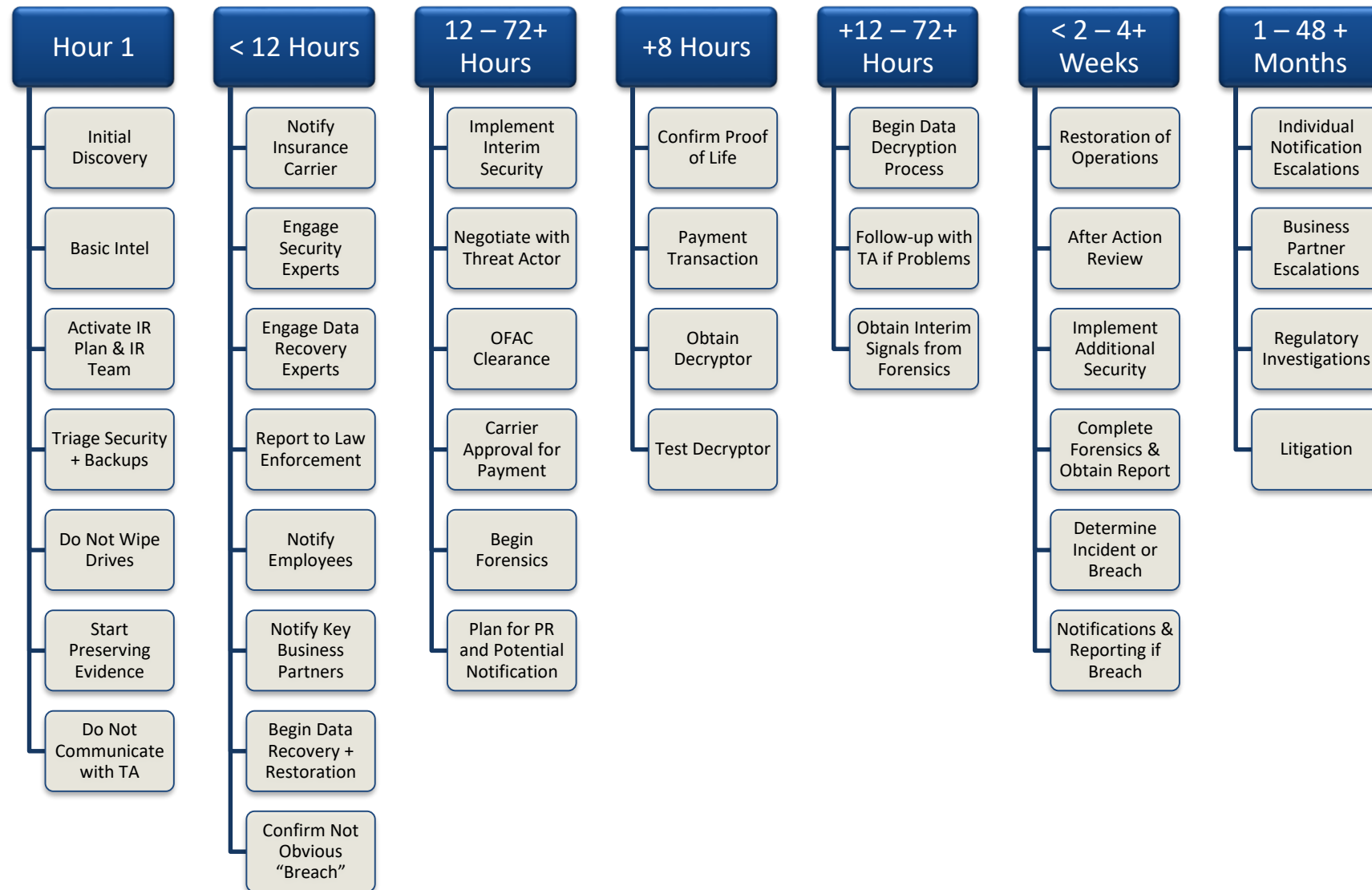
Ransomware response & recovery timeline



Ransomware response & recovery timeline



Ransomware response & recovery timeline

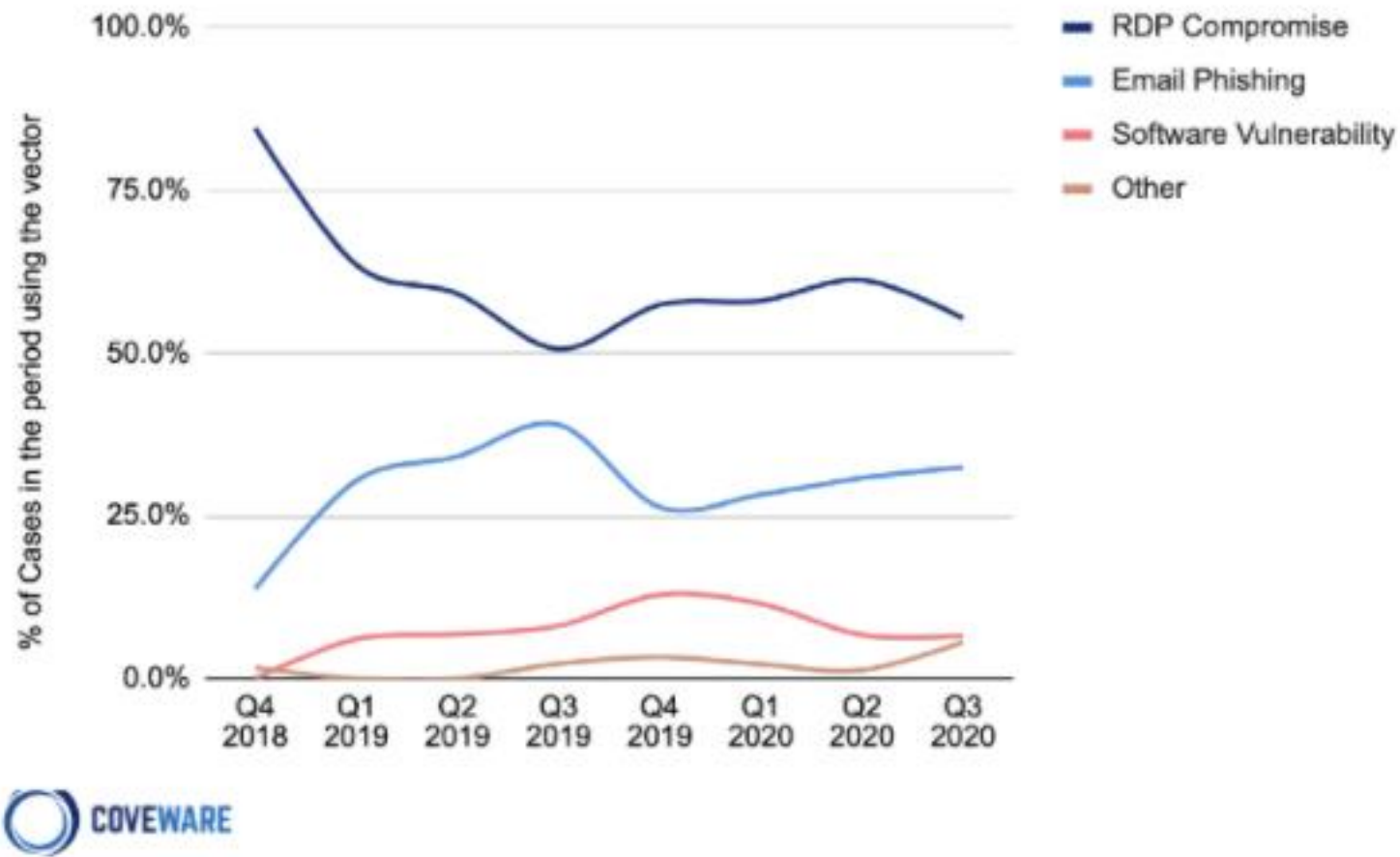


Recap: Preparation is the key to being able to do all of the things necessary for a successful response

Most common causes of ransomware attacks – and solutions for mitigating

Most common causes

Ransomware Attack Vectors



Source: <https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report>

Most common causes & solutions

RDP Access	<ul style="list-style-type: none">• This is random – scanning web for Internet facing RDP access• Virtual Private Network (VPN) with Multifactor Authentication (MFA)
Phishing	<ul style="list-style-type: none">• Email phishing tool• Workforce training and simulated phishing
Unpatched / Outdated Software	<ul style="list-style-type: none">• Install patches timely• No unsupported software
Passwords	<ul style="list-style-type: none">• Multifactor Authentication (MFA)• Longer passphrases
Backups, Backups, Backups!	<ul style="list-style-type: none">• 3-2-1 Backup Process• Something comparable – you may end up with only your offline backup

What we can do



SpencerFane

So, what are reasonable security measures or reasonable policies and procedures?

How 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.

How 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.

Cybersecurity best practices checklist

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
 - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature-based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Written incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Endpoint Detection & Response (EDR) Tool
17. Managed services provider (MSP) or managed security services provider (MSSP).
18. Cyber risk insurance.

Does your company have reasonable cybersecurity?

In re Target Data Security Breach Litigation, (Financial Institutions) (Dec. 2, 2014)
F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236 (3rd Cir. Aug. 24, 2015)



SpencerFane®

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
 - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature-based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Written incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Endpoint Detection & Response (EDR) Tool
17. Managed services provider (MSP) or managed security services provider (MSSP).
18. Cyber risk insurance.

Does your company have adequate internal network controls?



SpencerFane®

FTC v. LabMD, (July 2016 FTC Commission Order)

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
 - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature-based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Written incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Endpoint Detection & Response (EDR) Tool
17. Managed services provider (MSP) or managed security services provider (MSSP).
18. Cyber risk insurance.

Does your company have written policies and procedures focused on cybersecurity?



SpencerFane®

SEC v. R.T. Jones Capital Equities Mgt., Consent Order (Sept. 22, 2015)

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
 - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature-based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Written incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Endpoint Detection & Response (EDR) Tool
17. Managed services provider (MSP) or managed security services provider (MSSP).
18. Cyber risk insurance.

Does your company have a written cybersecurity incident response plan?



SpencerFane®

SEC v. R.T. Jones Capital Equities Mgt., Consent Order (Sept. 22, 2015)

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
 - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature-based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. **Written incident response plan.**
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. Third-party security risk management program.
15. Firewall, intrusion detection and prevention systems.
16. Endpoint Detection & Response (EDR) Tool
17. Managed services provider (MSP) or managed security services provider (MSSP).
18. Cyber risk insurance.

Does your company manage third party cyber risk?

In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014)

1. Risk assessment.
2. Policies and procedures focused on cybersecurity.
 - Social engineering, password, security questions
3. Training of all workforce on P&P, then security.
4. Phish all workforce (esp. leadership).
5. Multi-factor authentication.
6. Signature-based antivirus and malware detection.
7. Internal controls / access controls.
8. No outdated or unsupported software.
9. Security patch updates management policy.
10. Backups segmented offline, cloud, redundant.
11. Written incident response plan.
12. Encrypt sensitive and air-gap hypersensitive data.
13. Adequate logging and retention.
14. **Third-party security risk management program.**
15. Firewall, intrusion detection and prevention systems.
16. Endpoint Detection & Response (EDR) Tool
17. Managed services provider (MSP) or managed security services provider (MSSP).
18. Cyber risk insurance.

If the common causes and best practices are known why are companies are still getting hit because of them?

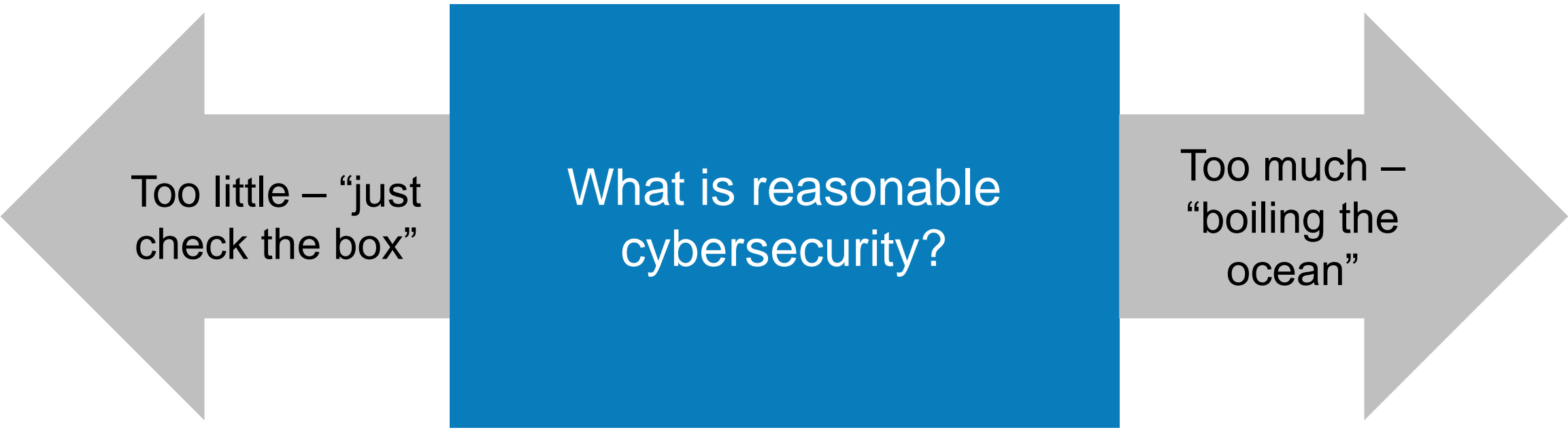
How we can do it



SpencerFane



How do you prioritize and
execute on all of these
things – at scale?



Too little – “just
check the box”

What is reasonable
cybersecurity?

Too much –
“boiling the
ocean”

How mature is the company's cyber & privacy risk management program?

- “GMR Transcription Services, Inc. . . . Shall . . . establish and implement, and thereafter maintain, a comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers.” **In re GMR Transcription Svcs, Inc., Consent Order (Aug. 14, 2014)**
- “We believe disclosures regarding a company’s cybersecurity risk management program and how the board of directors engages with management on cybersecurity issues allow investors to assess how a board of directors is discharging its risk oversight responsibility in this increasingly important area.” **SEC Statement and Guidance (Feb. 21, 2018)**
- “Each Covered Entity shall maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the Covered Entity’s Information Systems.” **NYDFS Cybersecurity Regulations § 500.02**
- “Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including ...” **GDPR, Art. 32**

How mature is the company's cyber & privacy risk management program?



- “GMR T
compre
confide
Transc
- “We be
of direc
director
and Gu
- “Each C
and ava
- “Taking
purpose
natural
measur

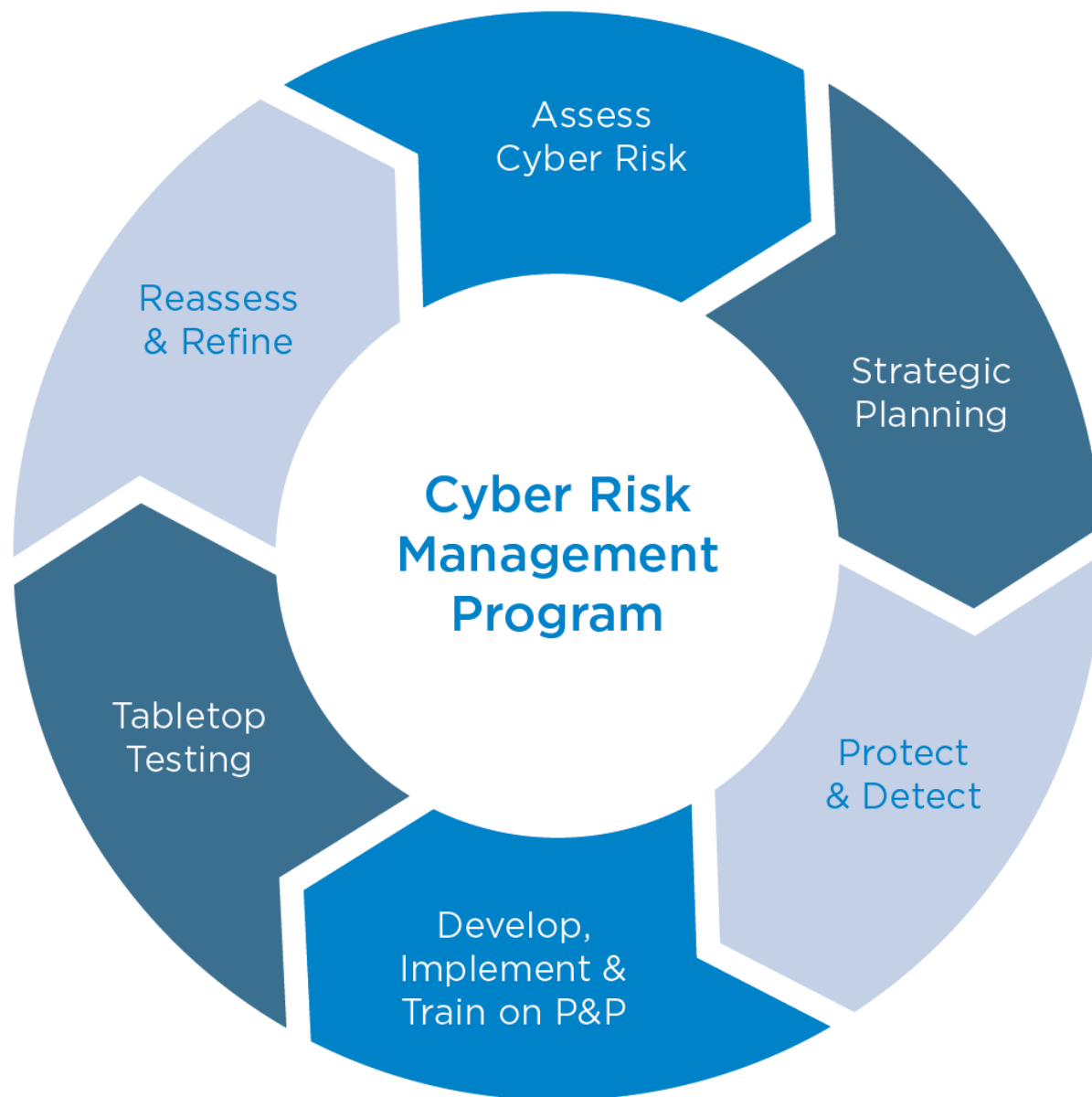
“A business **shall implement and maintain reasonable procedures**, including taking any appropriate corrective action, to protect from unlawful use or disclosure any **sensitive personal information** collected or maintained by the business in the regular course of business.”

– *Ken Paxton*

board
of
ment

tegrity
500.02

nd
s of
onal



Reasonable cybersecurity is a process, not a definition

Why have an attorney lead your risk management program?

Our role as attorneys is to provide legal advice regarding the legal, regulatory compliance, and overall defensibility of the company's current cyber risk and cybersecurity defense posture and then lead the company in developing, implementing, testing, and maturing a comprehensive cyber risk management program.

- In providing this legal advice, we will engage the services of other professionals – consulting experts – to assist us in evaluating the current status and moving towards a more defensible posture.
- Our work may be treated as attorney-client privileged and work-product, in certain situations.
- But, both attorney-client privilege and work-product are very uncertain in this environment and are certainly no guarantees.
- Communicate as though there will be no privilege.

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 risks²
- Use defensive infrastructure and policies and procedures to protect network and data^{1,2,3,4,5}
- Workforce training^{2,3}
- Detect events²
- Respond to events to mitigate negative impact²
- Recover from events to restore normalcy²
- Regularly review network activity such as audit logs, access reports, incident tracking reports³
- 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 Officer²

1. In re GMR Transcription Svcs, Inc., Consent Order (August 14, 2014)

2. NYDFS Cybersecurity Regulations Section 500.02

3. HIPAA Security Management Process, [§164.308\(a\)\(1\)\(ii\)](#)

4. SEC Statement and Guidance on 2/21/18

5. GDPR Art. 32


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.

“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*

Cyber risk management program – assessment



CONFIDENTIAL ATTORNEY-CLIENT PRIVILEGE

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

Cyber Risk Initial Assessment

Prepared for
[CLIENT]
("Client")

Date: December 20, 2021
Version: 1.0


Spencer Fane LLP | spencerfane.com

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



17. Does Client accept, process, store or transmit payment card information?
Click or tap here to enter text.

18. Is Client compliant with Payment Card Industry Data Security Standards?
Click or tap here to enter text.

4. Are Client's systems hosted internally, outsourced, or a hybrid? Please describe.
Click or tap here to enter text.

5. To what extent does Client use third party cloud services?
Click or tap here to enter text.

19. Does Client have logging enabled on all available systems? If so, how long are the logs retained?
Click or tap here to enter text.

20. What is Client's process for backing up its network and how are such backups stored and secured?
Click or tap here to enter text.

21. What is Client's process for verifying that its backups are both being completed and can be restored?
Click or tap here to enter text.

41. What concerns does Client have about its data, even if they do not rise to the level of a known risk?
Click or tap here to enter text.

42. Does Client have a data map that shows the flow of how all data enters the environment, is accessed, processed, and stored within the environment, and then exits the environment (including all third party and cloud based connections to the environment)?
Click or tap here to enter text.

Cyber risk management program – strategic planning

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 items that we need to complete for Phase 1 of this process, listed below:

Action Items	Status
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

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 items that we need to complete for Phase 1 of this process, listed below:

Action Items	Status
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)	
1.5.2.5. Data Classification	
1.5.2.6. Document Retention (see suggestions in draft with data	

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)	

How do we start preparing for incident response?

Incident response starts with preparing for resilience

There are two things that my experience has shown me to be absolutely critical to resilience that every company should have:

- Cyber insurance
 - This is what pays for you to do what you need to do for a proper response.
- Incident response planning
 - This how you know what to do, when to do it, who is doing what, and how.
 - Basic process:
 - Determine your leaders and key internal and external players
 - Get your preferred vendors pre-approved under your cyber insurance policy (or, get different policy)
 - Develop your IR plan
 - Including developing communications protocols and retention of external players (MSP, security/forensics, decryption, notification, public relations, legal)
 - Educate the players on their roles
 - IR Team practice through tabletop exercises
 - Refine and be prepared to execute when needed

Prepare for resilience: questions your breach coach wants you to ask now

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?
14. Have you performed After Action Reviews (AAR) and revised your IRP for lessons learned?



"Amateurs talk about tactics,
but professionals study
logistics."

- *Gen. Omar Bradley*

Cyber Incident Quick Reaction Sheet



SpencerFane®

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]		
IT MSP Provider	[External - MSSP / SOC Provider]		
	[External - Cybersecurity]		
	[External - Breach Counsel]	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
	Spencer Fane, LLP		
	Shawn Tuma		
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 248-207-8616 beleatherman@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

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]		
IT MSP Provider	[External - MSSP / SOC Provider]		
	[External - Cybersecurity]		
	[External - Breach Counsel]	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
	Spencer Fane, LLP		
	Shawn Tuma		
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 248-207-8616 beleatherman@fbi.gov
Human Resources Personnel			
Vice President of Operations			

Cyber Incident Quick Response



SpencerFane®

Cyber Incident Quick Reaction Sheet

Title	Company	Contact
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]	d 972.321.2147 shuma@spencerfane.com
IT MSP Provider		
MSSP / SOC Provider		
Cloud Services Provider		
Breach Counsel	Spencer Fane LLP	Shawn Tuma d 972.321.2147 shuma@spencerfane.com
Cyber Insurance Carrier, Policy # and Policy location		
Cyber Insurance Broker		
Cybersecurity / Cyber Forensics Vendor		
Decryption/Negotiation Vendor		
FBI Contact		Richard Murray d 972.559.6100 m 505.948.6100 rmurray@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.com
Key Notes & Information		

Spencer Fane LLP | spencerfane.com

060AADBAB99677
24A3E01EDDCA12F
4E6.locky

060AADBAB99677
24FCA5244AC885E
677.locky

060AADBAB99677
24094AC08D9CB9
4141.locky

060AADBAB99677
24D34E78B5C1A0
9F1C.locky

060AADBAB99677
2402ABA49978DD
10B6.locky

060AADBAB99677
242783760BFAB23
748.locky

060AADBAB99677
24DB8A2C071883
DBDD.locky

060AADBAB99677
24069B58F2F5723
113.locky

_Locky_recover_
instructions.txt

Backup Contact Information

my Rucker
4.459.5880
7.821.5002
er@spencerfane.com

y Rucker
459.5880
821.5002
@spencerfane.com

herman
-5132
-8616
an@fbi.gov

Cyber Incident Quick Reaction Sheet



SpencerFane®

Cyber Incident Quick Reaction Sheet

Title	Company	Contact
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]	d 972.321.2147 shawn@spencerfane.com
Shawn Tuma		
IT MSP Provider		
MSSP / SOC Provider		
Cloud Services Provider		
Breach Counsel	Spencer Fane LLP	Shawn Tuma d 972.321.2147 shawn@spencerfane.com
Cyber Insurance Carrier		
Policy # and Policy location		
Cyber Insurance Broker		
Cybersecurity / Cyber Forensics Vendor		
Decryption/Negotiation Vendor		
FBI Contact		Richard Murray d 972.559.5132 m 505.948.6132 rmurray@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.com
Key Notes & Information		

Spencer Fane LLP | spencerfane.com

1. Take a picture and save in phone
2. Start a text group now

Backup Contact Information

my Rucker
4.459.5880
7.821.5002
er@spencerfane.com

y Rucker
459.5880
821.5002
@spencerfane.com

herman
-5132
-8618
an@fbi.gov

_Locky_recover_
instructions.txt



Shawn Tuma

Co-Chair, Cybersecurity & Data Privacy

Spencer Fane LLP

972.324.0317

stuma@spencerfane.com



SpencerFane®

- 20+ Years of Cyber Law Experience
- Practitioner Editor, Bloomberg BNA – Texas Cybersecurity & Data Privacy Law
- Council Member, Southern Methodist University Cybersecurity Advisory
- Board of Advisors, North Texas Cyber Forensics Lab
- Policy Council, National Technology Security Coalition
- Board of Advisors, Cyber Future Foundation
- Cybersecurity & Data Privacy Law Trailblazers, National Law Journal (2016)
- SuperLawyers Top 100 Lawyers in Dallas (2016)
- SuperLawyers 2015-21
- Best Lawyers in Dallas 2014-21, D Magazine
- Past Chair, Computer & Technology Section, State Bar of Texas
- Privacy and Data Security Committee of the State Bar of Texas
- College of the State Bar of Texas
- Fmr Board of Directors, Collin County Bench Bar Conference
- Past Chair, Civil Litigation & Appellate Section, Collin County Bar Association
- Information Security Committee of the Section on Science & Technology Committee of the American Bar Association
- North Texas Crime Commission, Cybercrime Committee & Infragard (FBI)
- International Association of Privacy Professionals (IAPP)