



Frankfurt Kurnit Klein+Selz PC

Cyber Insurance Trends and Predictions

Impacts of Regulatory Changes, Threats, and Cyber Insurance

Rick Borden, Frankfurt Kurnit Klein & Selz

Doug Howard, CEO Pondurance



Disclosure

These materials are provided by Frankfurt Kurnit and Pondurance and reflect information as of the date of presentation.

The contents are not legal advice and are intended to provide a general guide to the subject matter only and should not be treated as a substitute for specific advice concerning individual situations.

You may not copy or modify the materials or use them for any purpose without our express prior written permission.

SEC Rule Proposals

- Investment Adviser Rules
- Broker-Dealer and Market Participant Rules
- Regulation S-P
- Reg SCI
- Outsourcing Rule

SEC PUBLIC COMPANY CYBER RULE

- Board and Officer Cyber Expertise
- Policies and Procedures
- Risk Factors
- Business Description
- MD&A
- Material Events

SEC PUBLIC COMPANY CYBER RULE

- Board and Officer Cyber Expertise
- Policies and Procedures
- Risk Factors
- Business Description
- MD&A
- Material Events

CURRENT CYBERSECURITY LAWS, RULES, AND REGULATIONS

Federal Laws:

- SEC Rules
- Bank Secrecy Act
- FISMA & CISA
- GLBA
 - FTC Safeguards Rule
 - SEC Regulation S-P
- FTC Unfair & Deceptive Trade Practices

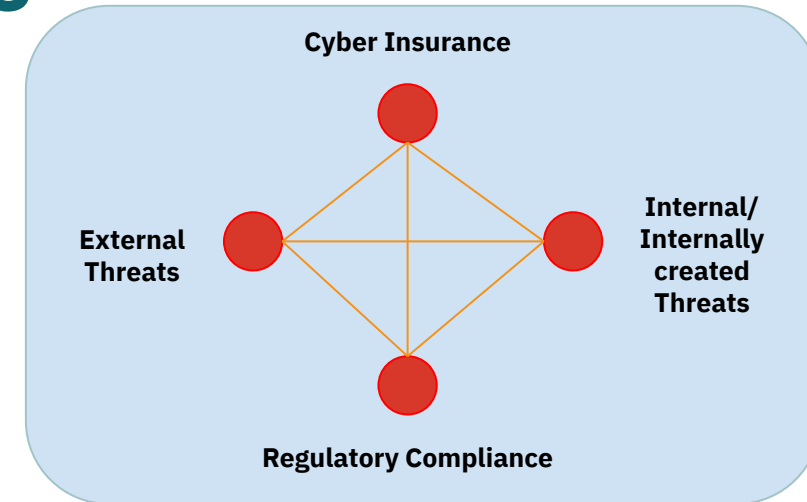
State Laws:

- [New York] NY DFS / NY SHIELD
- [California] CCPA / CPRA
- [Massachusetts] 201 CMR 17
- [Connecticut] Public Act 59
- [Ohio] Data Protection Act
- Various State Unfair & Deceptive Trade Practices

Cyber Insurance Trends and Predictions

Threat Landscape

- Hygiene and lack of monitoring
- GeoPolitical/Nation State sophisticated Attacks (APT)
- Unauthorized Access (Insider/External User, Network, System)
- Vulnerabilities
- Lack of data mapping and location awareness
- Poor User guardrails and trainings
- Regulatory Compliance



Cyber Insurance Market Influences

- General policy that include Cyber Insurance and Cyber Insurance Claim Rates
- Causes for Cyber Insurance Claims (drives minimum requirements [currently Ransomware Supplement])
- Anticipation of future threat impacts

Top Cyber Threats and Fraud

Account Takeover	Compromised Credentials	DoS Attack	Open Redirection	Social Engineering Attack
Advanced Persistent Threat	Credential Dumping	Drive-by Download Attack	Pass the Hash	Spyware
AWS Attacks	Credential Reuse Attack	Insider Threat	Phishing (Payloads, Spear, Whale)	SQL Injection
Application Access Token	Credential Stuffing	IoT Threats	Password Spraying	Supply Chain Attack
Bill Fraud	Cross-Site Scripting	IoMT Threats	Privileged User Compromise	System Misconfiguration
Brute Force Attack	Crypto Jacking	Macro Viruses	Ransomware	Zoom Child Processing
Business Invoice Fraud	Data from Information Repositories	Malicious Powershell	Ransomware as a service	Typosquatting
Cloud Access Management	DDoS Attack	Man-in-the-Middle Attack	Router and Infrastructure Compromise	Water hole attack
Cloud Crypto Mining	Disabling Security Tools	Masquerade Attack	Shadow IT	Wire Attack
Command and Control	DNS Attacks (Hijacking, Tunneling, Amplification)	Meltdown and Spectre Attack	Service Account Compromise	Zero-Day Exploit
		Networking Sniffing	Simjacking	

Anatomy of a Breach

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 40 techniques	Credential Access 15 techniques	Discovery 29 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 12 techniques
Active Scanning (2)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (2)	Account Manipulation (4)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (2)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (2)	Application Layer Protocol (4)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Compromise Accounts (2)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (3)	Access Token Manipulation (3)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (2)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	Boot or Logon Autostart Execution (15)	Credentials from Password Stores (3)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (4)	Develop Capabilities (4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (2)	Exfiltration Over C2 Channel	Data Manipulation (2)
Gather Victim Org Information (4)	Establish Accounts (2)	Phishing (3)	Inter-Process Communication (2)	Browser Extensions	Browser Extensions	Browser Extensions	Forced Authentication	Cloud Service Dashboard	Remote Services (6)	Browser Session Hijacking	Dynamic Resolution (2)	Defacement (2)	Defacement (2)
Phishing for Information (2)	Obtain Capabilities (3)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Create or Modify System Process (4)	Create or Modify System Process (4)	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Other Network Medium (1)	Disk Wipe (2)
Search Closed Sources (2)	Stage Capabilities (3)	Supply Chain Compromise (2)	Scheduled Task/Job (4)	Scheduled Task/Job (4)	Domain Policy Modification (2)	Domain Policy Modification (2)	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage Object	Fallback Channels	Exfiltration Over Physical Medium (1)	Endpoint Denial of Service (4)
Search Open Technical Databases (3)		Trusted Relationship	Shared Modules	Create Account (2)	Domain Policy Modification (2)	Execution Guardrails (1)	Modify Authentication Process (4)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Exfiltration Over Web Service (2)	Firmware Corruption
Search Open Websites/Domains (2)		Valid Accounts (4)	Software Deployment Tools	Create or Modify System Process (4)	Escape to Host	Exploitation for Defense Evasion	Network Sniffing	Domain Trust Discovery	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Exfiltration Over Web Service (2)	Inhibit System Recovery
Search Victim-Owned Websites			System Services (2)	Event Triggered Execution (18)	Event Triggered Execution (18)	File and Directory Permissions Modification (2)	OS Credential Dumping (3)	File and Directory Discovery		Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (2)
			User Execution (2)	External Remote Services	Exploitation for Privilege Escalation	Hide Artifacts (3)	Steal Application Access Token	Group Policy Discovery		Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
			Windows Management Instrumentation	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Hijack Execution Flow (11)	Steal or Forge Kerberos Tickets (4)	Network Service Scanning		Data from Removable Media	Protocol Tunneling		Service Stop
				Implant Internal Image	Process Injection (11)	Impair Defenses (3)	Steal Web Session Cookie	Network Share Discovery		Data Staged (2)	Proxy (4)		System Shutdown/Reboot
				Modify Authentication Process (4)	Indicator Removal on Host (3)	Indicator Removal on Host (3)	Two-Factor Authentication Interception	Network Sniffing		Email Collection (2)	Remote Access Software		
				Office Application Startup (4)	Indirect Command Execution	Indirect Command Execution	Unsecured Credentials (7)	Password Policy Discovery		Input Capture (4)	Traffic Signaling (1)		
				Pre-OS Boot (3)	Masquerading (7)	Masquerading (7)		Peripheral Device Discovery		Screen Capture	Web Service (2)		
				Scheduled Task/Job (8)	Modify Authentication Process (4)	Modify Authentication Process (4)		Permission Groups Discovery (3)		Video Capture			
				Server Software Component (4)	Modify Cloud Compute Infrastructure (4)	Modify Cloud Compute Infrastructure (4)		Process Discovery					
				Traffic Signaling (1)	Modify Registry	Modify Registry		Query Registry					
				Valid Accounts (4)	Modify System Image (2)	Modify System Image (2)		Remote System Discovery					
					Network Boundary Bridging (1)	Network Boundary Bridging (1)		Software Discovery (1)					
					Obfuscated Files or Information (3)	Obfuscated Files or Information (3)		System Information Discovery					
					Pre-OS Boot (3)	Pre-OS Boot (3)		System Location Discovery (1)					
					Process Injection (11)	Process Injection (11)		System Network Configuration Discovery (1)					
					Reflective Code Loading	Reflective Code Loading		System Network Connections Discovery					
					Rogue Domain Controller	Rogue Domain Controller		System Owner/User Discovery					
					Rootkit	Rootkit		System Service Discovery					
					Signed Binary Proxy Execution (13)	Signed Binary Proxy Execution (13)		System Time Discovery					
					Signed Script Proxy Execution (1)	Signed Script Proxy Execution (1)		Virtualization/Sandbox Evasion (2)					
					Subvert Trust Controls (3)	Subvert Trust Controls (3)							

Cyber Insurance Trends and Predictions

Historic Influences

Security Threat	Resulting Cyber Insurance Requirement
Ransomware	Backups, Endpoint Detection and Response (EDR) /Managed Endpoint Detection and Response (MDR)
Business Email Compromise	MFA, 24/7 Monitoring
Credential Compromise	Multi-Factor Authentication
AD Service Account Compromise	Reduction in service accounts/high degree of security of systems and access/MFA
Privileged Account Compromise	24/7 logging and monitoring of Privileged Account Escalations
User Awareness Training	User Training, Testing and Phishing Testing
System and Software Vulnerabilities	Vulnerability Scanning and Patch Management
User Errors	Awareness Training
Lack of System Inventory	Basic system inventory and active awareness/MAC Management



Evolving Threats: Russia



Hackers have taken sides:

- Those that support Ukraine
- Those that support Russia

-
- Russia has hired the Russia aligned malware developers and contractors to launch attacks against 0-day attacks:
 - USA Targets (military, financial, infrastructure)
 - Companies that have withdrawn from Russia
<https://som.yale.edu/story/2022/over-400-companies-have-withdrawn-russia-some-remain>
 - US Government continues to walk the line between acts of war and cyber



Frankfurt Kurnit Klein+Selz PC

Suspected Breach



What Would Make You Think You Have a Breach?

The obvious

- You get a ransom demand
- You receive notice from law enforcement or a service provider
- You receive an alert by a third-party
- You detect it

Suspicion and the less obvious

- System performance
- Dark Web data

Did Data Get Exfiltrated?

The obvious

- Proof and disclosure by the offender
- Notification by a third-party
- Real-time alerting (MDR, SIEM, DLP)
- Audit Records/DFIR Analysis

Suspicion and the less obvious

- Has it likely been stolen given the situation
- Claims by the offender, but no sample proof
- System access but no audit records
- Logical exposure scenario
- Dark Web data

Anatomy of a Breach



Anatomy of a Breach

COMMAND and CONTROL
Finalize continuous access to target systems and plan for undetected exfiltration

COLLECTION
Identify ways to collect data for exfiltration and ways to access and encrypt data (Ransomware)

LATERAL MOVEMENT
Expand to high value targets or jump points to high value targets

DISCOVERY
Identify high value data for extraction and encryption (Ransomware)



RECONNAISSANCE and RESOURCE DEVELOPMENT
Identification of weaknesses or broadly known weaknesses and associated tool developments to exploit weakness

ACCESS
Gaining access into a target environment without detection

EXECUTION, PERSISTENCE, PRIVILEGED ESCALATION, and CREDENTIAL ACCESS
Now establish an undetected landing point in which to expand from and identify ways to expand from the entry point

DEFENSE EVASION
Continually limit activities and expansion of access and footprint in ways they look like normal traffic or are undetectable

We Have a Breach

What are your priorities in responding to a breach?



Risk to your revenues/mission



Risk to your reputation



Risk to your regulatory requirements



Risk to your safety



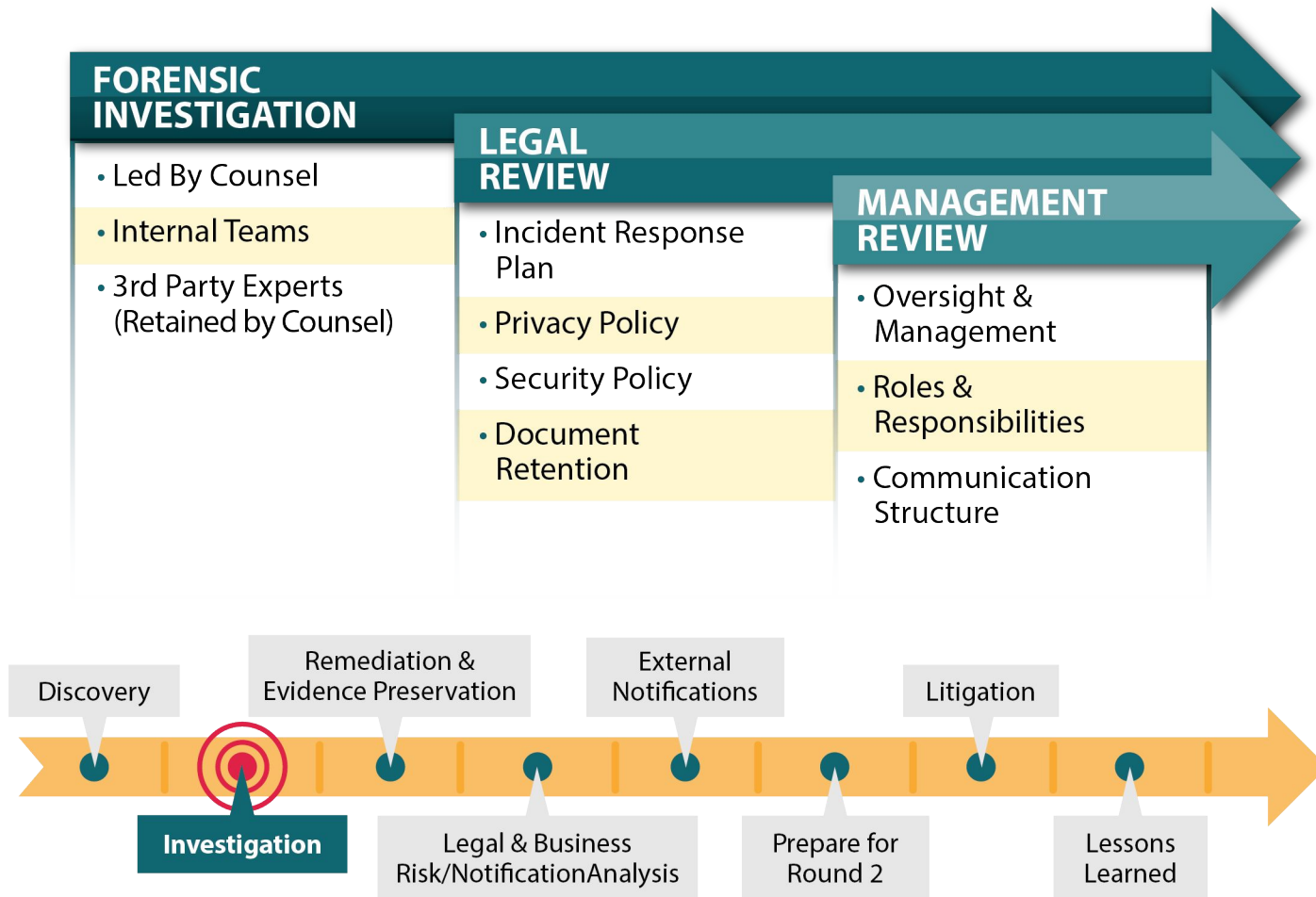
Frankfurt Kurnit Klein + Selz PC

Anatomy



Investigation and Validation

UNDERSTANDING THE BREACH

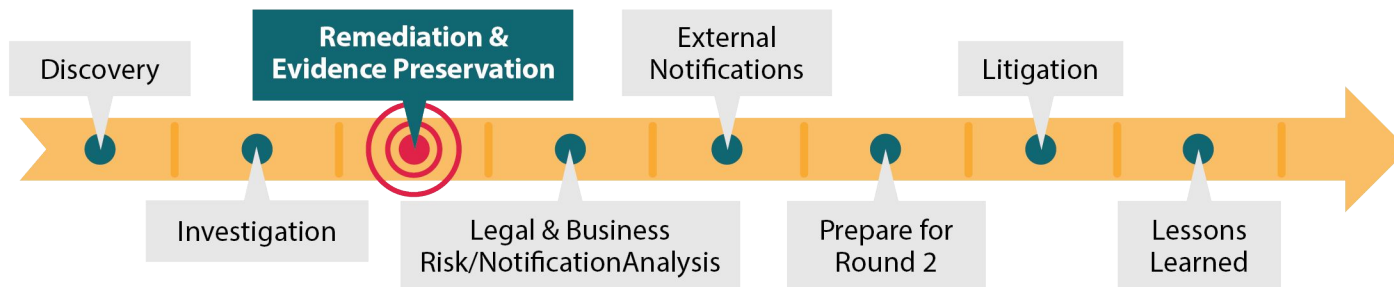
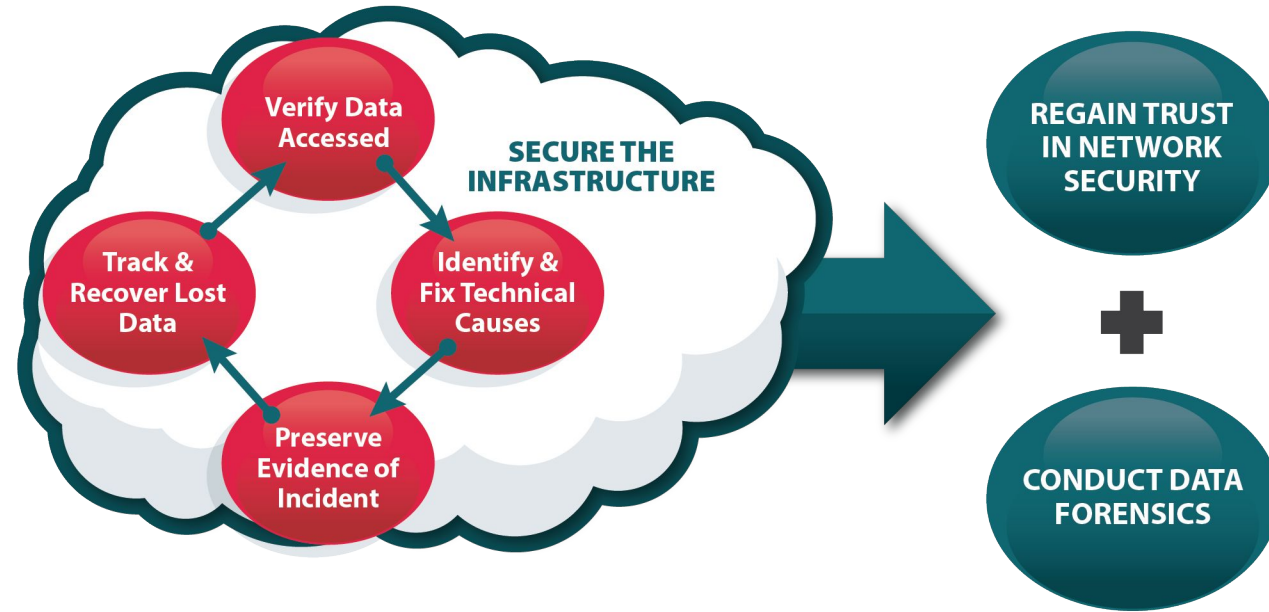


Investigation

- Validation of breach
- Let legal be your protective umbrella
- Relative peer comparison and meeting minimal requirements
- Roles & responsibilities of active parties

Remedies & Preservation of Evidence

UNDERSTANDING THE BREACH



Remediation/Evidence Preservation

Root Cause Analysis and Remediation

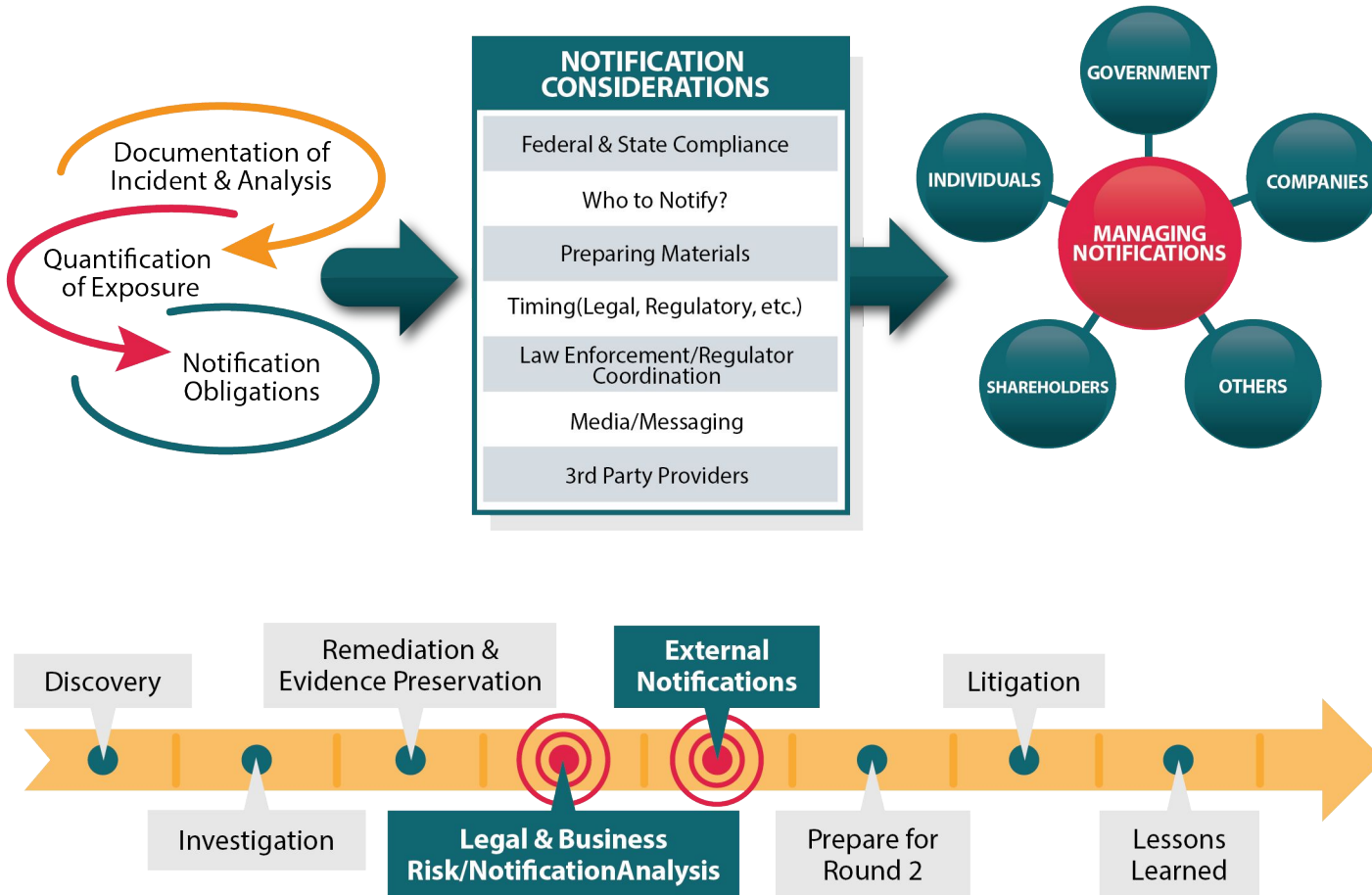
- Classification of data compromised
- Where is it
- What are the routes and dependent systems to access data
- Who has access and controls in place
- Visibility in place
- Remediation capabilities

Preserve evidence quickly

Communicate – frequently... and confidently when appropriate

Legal & Risk Analysis and Notification Requirements

UNDERSTANDING THE BREACH



Compliance & Risk Analysis

Privilege

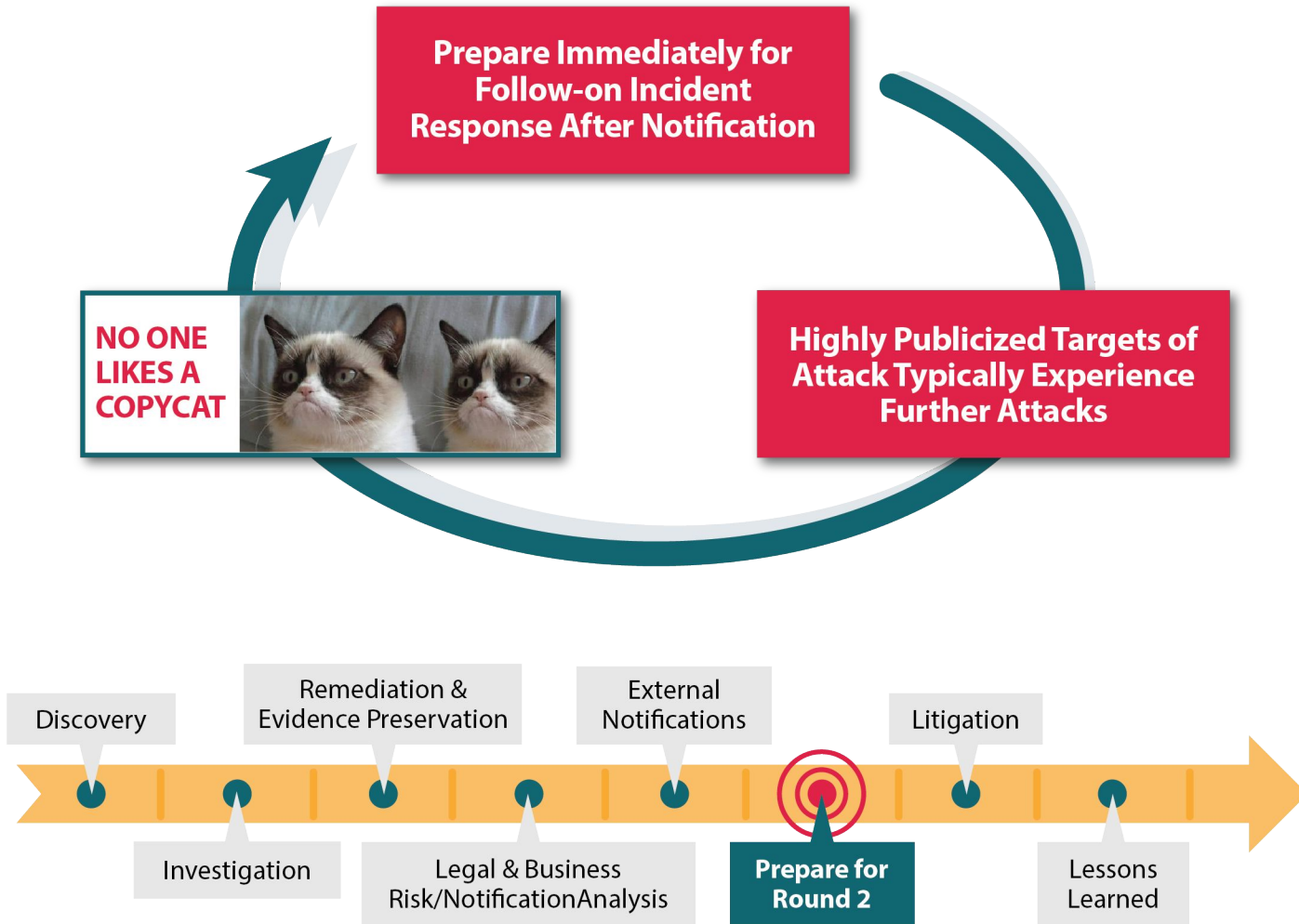
Notification Compliance

Communications Plan (internal/external)

- Consider other points of view
- Don't forget about your employees

Documentation

ROUND 2 – Here It Comes Again



Be prepared... *immediately*

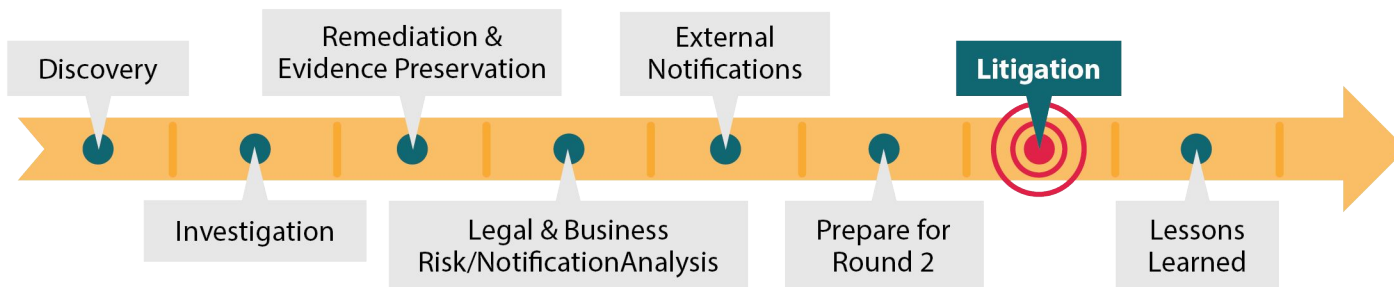
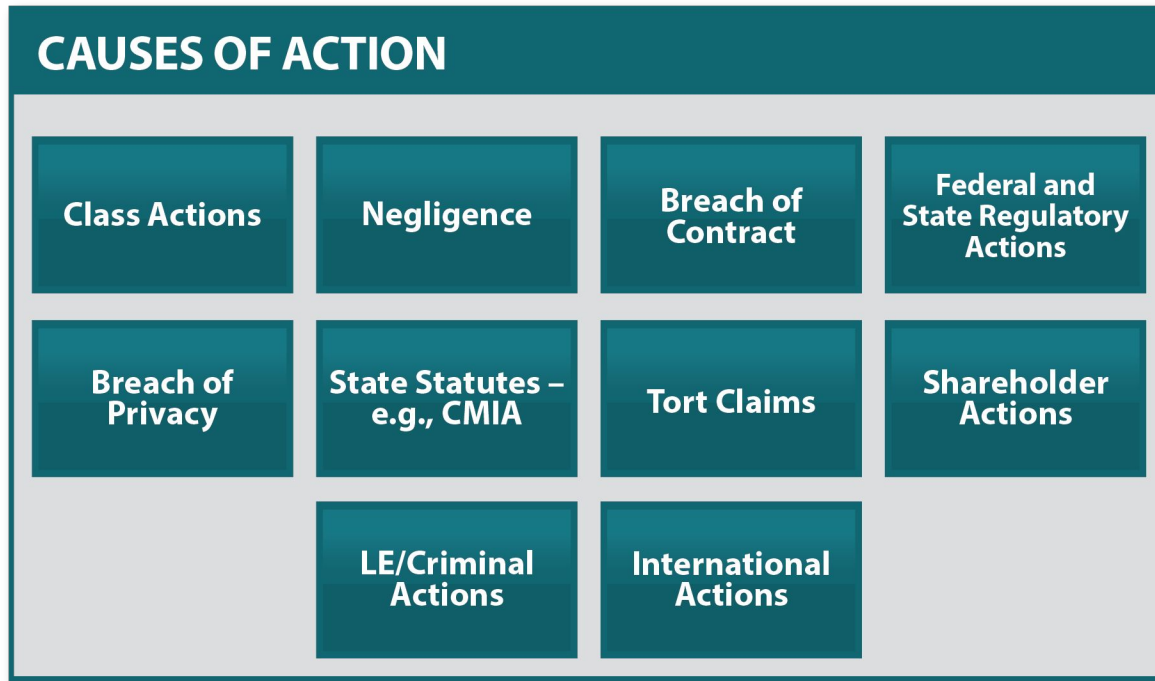
Warn employees to be prepared

Areas of improvements, failures, friction and risk

Areas to reduce remediation time during next breach

- Technologies
- People - Roles and responsibilities
- Processes - What to do, when to do it, and how to do it ... actions by roles and responsibility

Properly controlled information access



Litigation

- Industry fines and activities
- Customer actions
- Employees actions
- Legal mitigation



What should we have done?

What did we learn?

Is there a simple answer?

Simplified Recommendation



Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.

Simplified Recommendation



Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.

Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized

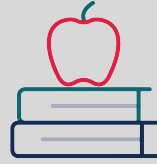
Simplified Recommendation



Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.

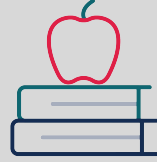


Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized



Communications and User Awareness Training and continuous role playing is critical. **You can reduce risk for the average user.** 1) train and test, 2) leverage email gateways, 3) Weed out the dummies and address, 4) Phish and Phish

Simplified Recommendation



Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.

Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized

Communications and User Awareness Training and continuous role playing is critical. **You can reduce risk for the average user.**
1) train and test, 2) leverage email gateways, 3) Weed out the dummies and address 4) Phish and Phish

Modernize your 24/7 detection capabilities with MDR/MxDR. Threats are 24/7, so must be your detection and response capabilities.

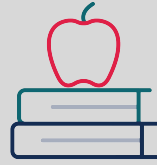
Simplified Recommendation



Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.



Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized



Communications and User Awareness Training and continuous role playing is critical. **You can reduce risk for the average user.** 1) train and test, 2) leverage email gateways, 3) Weed out the dummies and address 4) Phish and Phish

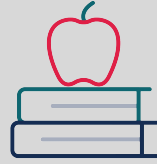


Modernize your 24/7 detection capabilities with MDR/MxDR. Threats are 24/7, so must be your detection and response capabilities.



Malware is not going anywhere. We assume you have client-based anti-virus running, which is a start. **Enrich AV** with **network malware detection, sandboxing technologies and application whitelisting.**

Simplified Recommendation



Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.

Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized

Communications and User Awareness Training and continuous role playing is critical. **You can reduce risk for the average user.** 1) train and test, 2) leverage email gateways, 3) Weed out the dummies and address, 4) Phish and Phish

Modernize your 24/7 detection capabilities with MDR/MxDR. Threats are 24/7, so must be your detection and response capabilities.

Malware is not going anywhere. We assume you have client-based anti-virus running, which is a start. **Enrich AV** with **network malware detection,** **sandboxing technologies** and **application whitelisting.**

Containerize and Encrypt all mobile devices! 1) Be careful to understand what MDMs do and don't do, 2) understand BYOD tradeoffs, 3) forecast – a reckoning is coming within mobile 3) containerize confidential data

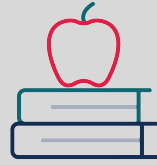
Simplified Recommendation



Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.



Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized



Communications and User Awareness Training and continuous role playing is critical. **You can reduce risk for the average user.** 1) train and test, 2) leverage email gateways, 3) Weed out the dummies and address, 4) Phish and Phish



Modernize your 24/7 detection capabilities with MDR/MxDR. Threats are 24/7, so must be your detection and response capabilities.



Malware is not going anywhere. We assume you have client-based anti-virus running, which is a start. **Enrich AV** with **network malware detection,** **sandboxing technologies** and **application whitelisting.**



Containerize and Encrypt all mobile devices! 1) Be careful to understand what MDMs do and don't do, 2) understand BYOD tradeoffs, 3) forecast – a reckoning is coming within mobile 3) containerize confidential data



Threat Intelligence if operationalized is powerful. 1) If it's in the news, it's probably too late, 2) customer specific intel and monitoring is critical, 3) A key is knowing what the next looming threat might look like and how to plan, recognize, respond and mitigate it as necessary.

Simplified Recommendation



Frankfurt Kurnit Klein+Selz PC

Continually progress forward with a plan by understanding your gaps.

Identify and prioritize known area of weaknesses. Have a plan and execute... moving forward is better than paralysis through analysis.

Continual Cyber Risk Reduction

Policy and Control Management

Controls should support Policies and context starts with Business Context.

- Business Risk
 - Safety
 - Reputation
 - Regulation
 - Revenue/Mission
- What gaps exist in what you documented you do verse operationally what you really do

Contextual Management

- IT Inventory
- Vulnerability Status
- Penetration Testing
- User Risk

Threat and IOC Awareness

- Threat Intel with Indicators of Compromise
- Realtime Surface Awareness
- Reverse Engineering and IOC Threat Analysis
- Honeypot



Frankfurt Kurnit Klein + Selz PC

Questions?



Thank You!

Frankfurt Kurnit Klein + Selz PC

