PONDURANCE

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

Frankfurt Kurnit Klein + Selz PC

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

PONDURANCE

# SEC PUBLIC COMPANY CYBER RULE

Frankfurt Kurnit Klein + Selz PC

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

PONDURANCE

# CURRENT CYBERSECURITY LAWS, RULES, AND REGULATIONS

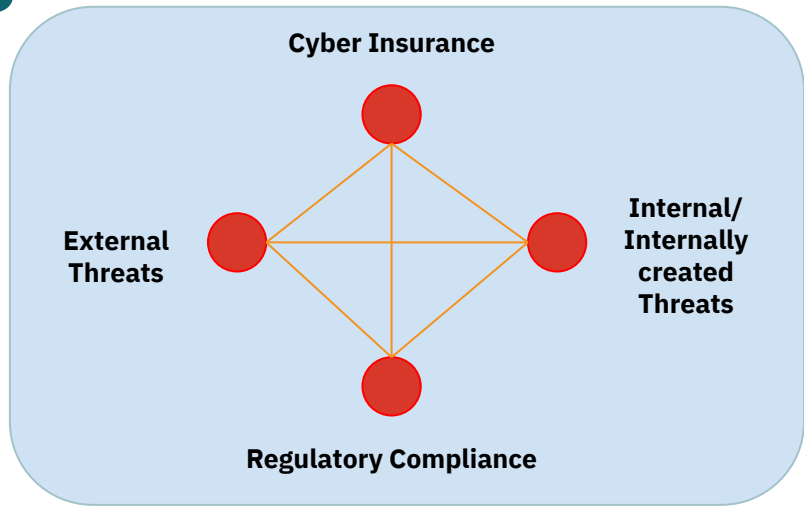
## Federal Laws:

- 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

PONDURANCE

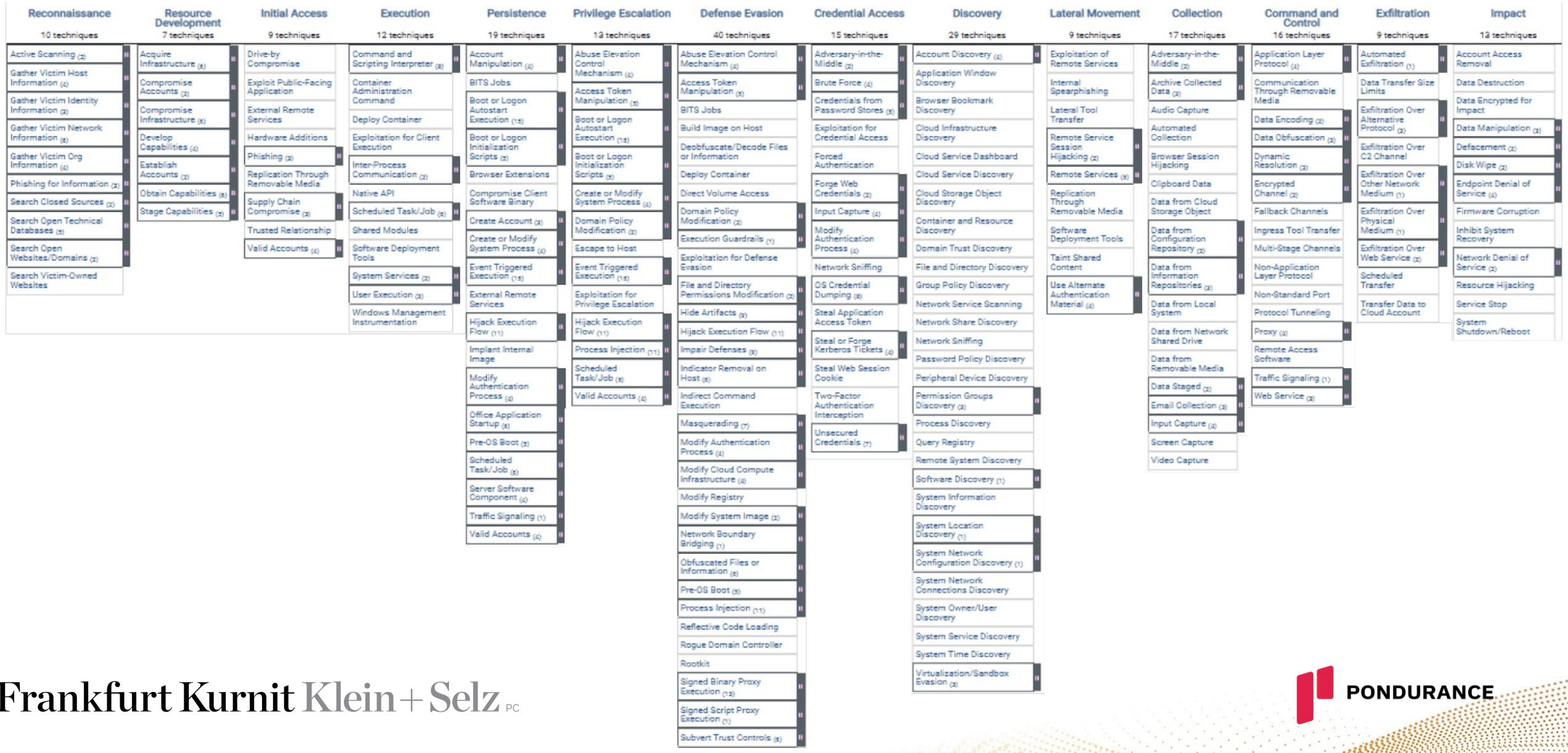
# Top Cyber Threats and Fraud

Frankfurt Kurnit Klein + Selz PC

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

PONDURANCE

# Anatomy of a Breach




Frankfurt Kurnit Klein + Selz PC

PONDURANCE

# 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 |

PONDURANCE

# Evolving Threats: Russia

Frankfurt Kurnit Klein + Selz PC

## 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

PONDURANCE

PONDURANCE

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?

Frankfurt Kurnit Klein + Selz PC

**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

PONDURANCE

# Anatomy of a Breach

# Anatomy of a Breach

Frankfurt Kurnit Klein+Selz PC

**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, PRIVILEDGED 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

PONDURANCE

# We Have a Breach

*What are your priorities in responding to a breach?*

Frankfurt Kurnit Klein + Selz PC

Risk to your revenues/mission

Risk to your reputation

Risk to your regulatory requirements

Risk to your safety

PONDURANCE

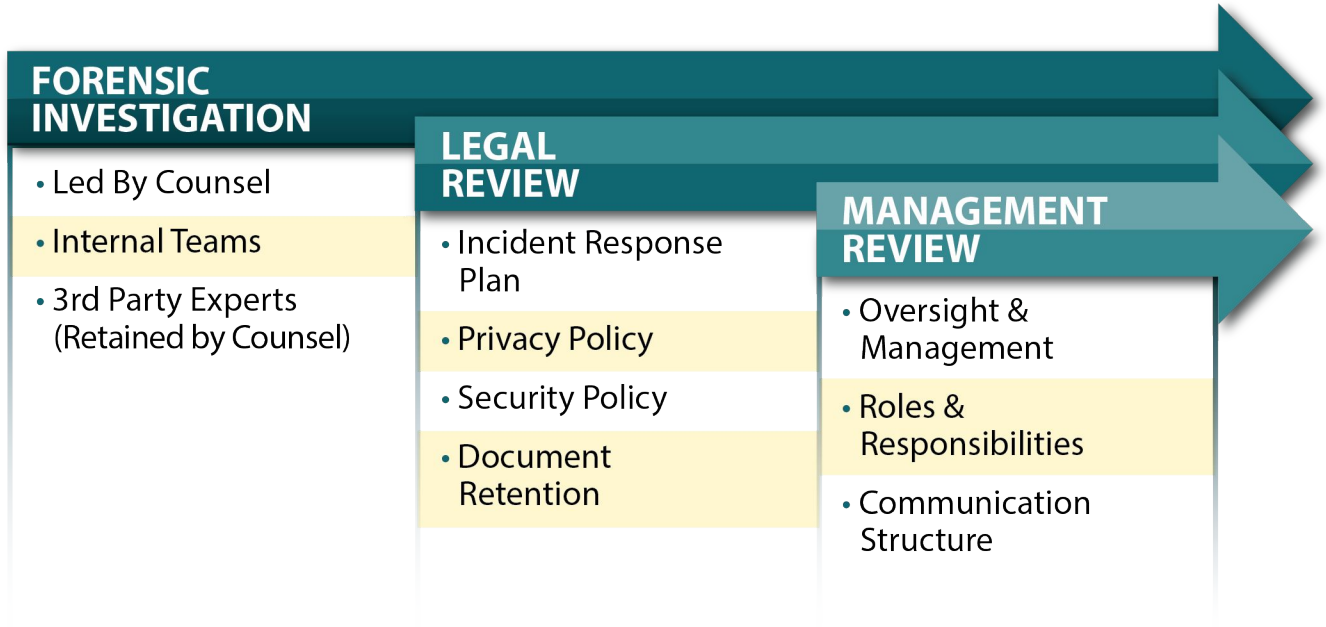
PONDURANCE

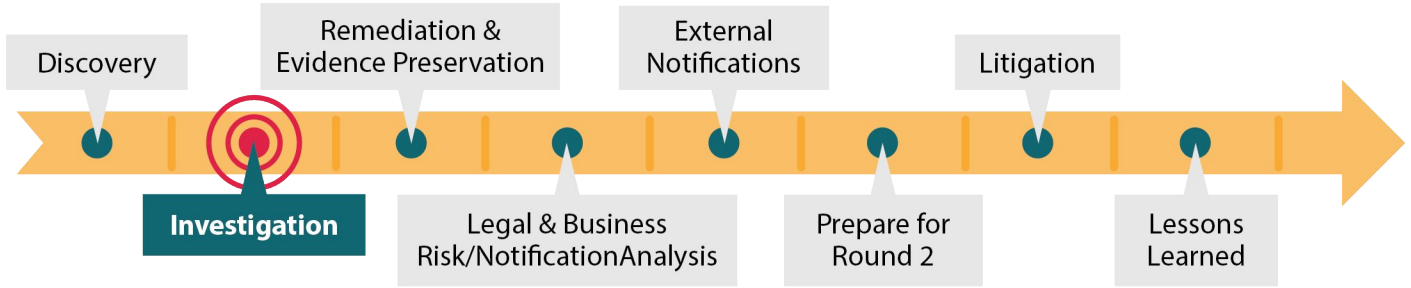
Frankfurt Kurnit Klein + Selz PC

# Anatomy

# Investigation and Validation

## UNDERSTANDING THE BREACH




Frankfurt Kurnit Klein+Selz PC

## Investigation

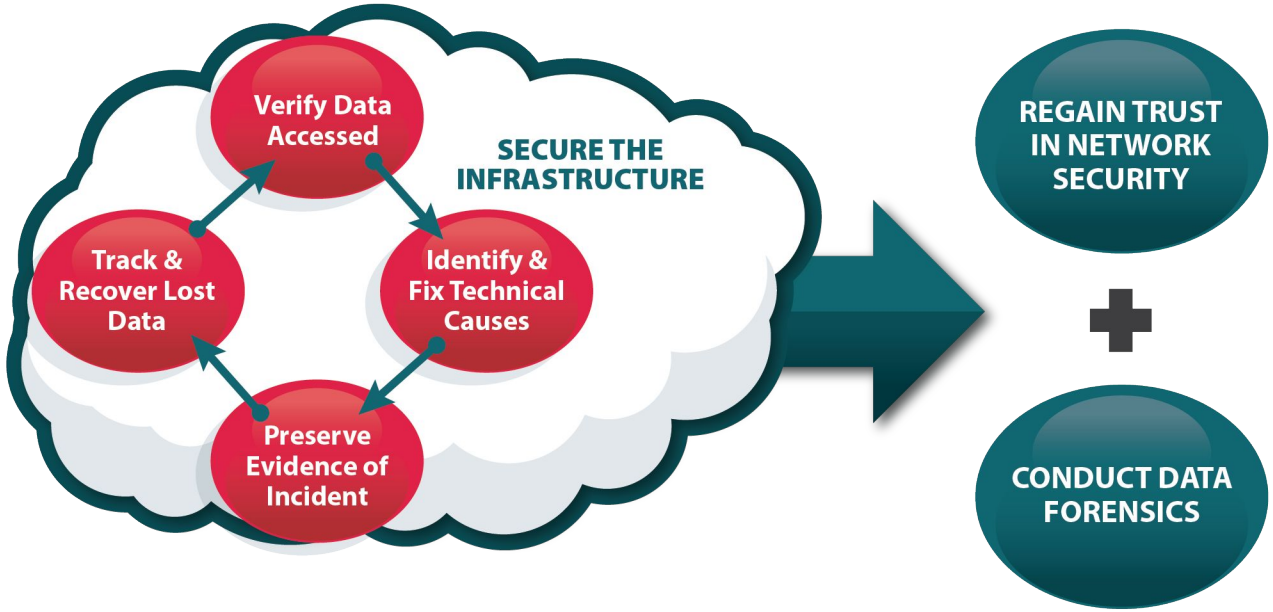
- Validation of breach
- Let legal be your protective umbrella
- Relative peer comparison and meeting minimal requirements
- Roles & responsibilities of active parties

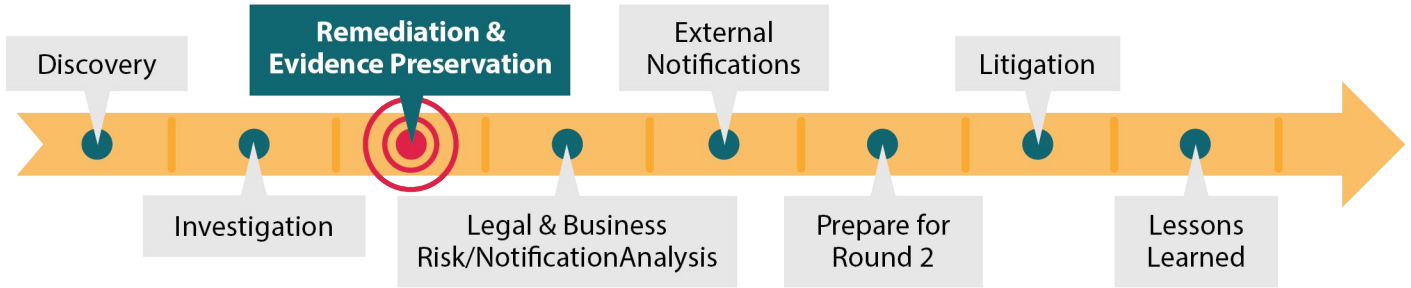
PONDURANCE

# Remedies & Preservation of Evidence

Frankfurt Kurnit Klein + Selz PC

## 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

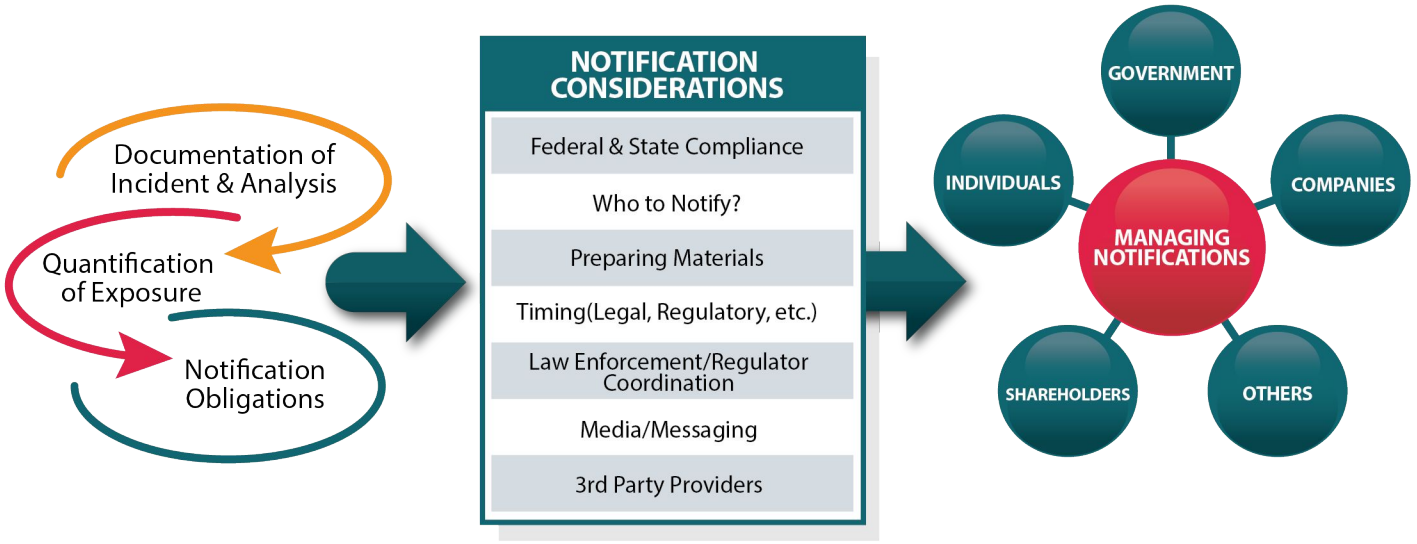
**Preserve evidence quickly**

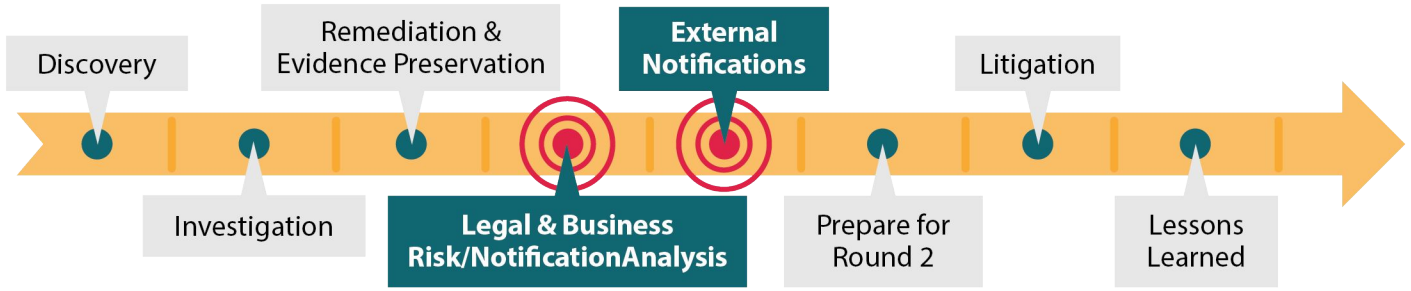
**Communicate – frequently… and confidently when appropriate**

# Legal & Risk Analysis and Notification Requirements

Frankfurt Kurnit Klein + Selz PC

## UNDERSTANDING THE BREACH




## Compliance & Risk Analysis

### Privilege

### Notification Compliance

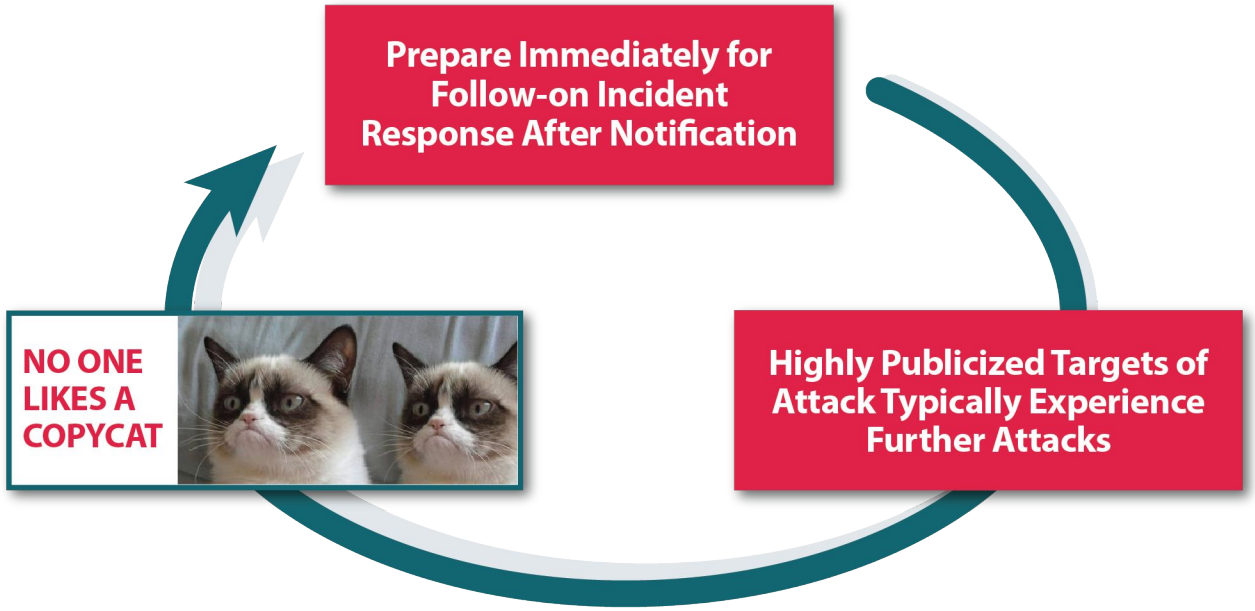
### Communications Plan (internal/external)

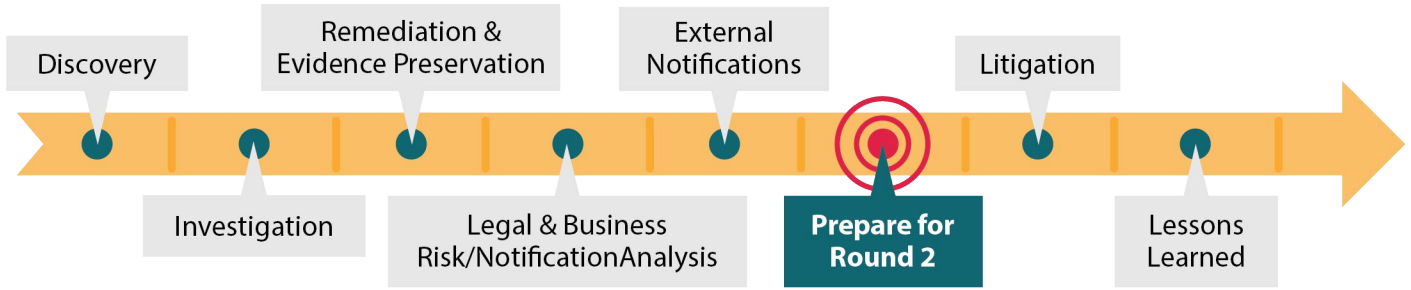
- Consider other points of view
- Don't forget about your employees

### Documentation

# ROUND 2 – *Here It Comes Again*

Frankfurt Kurnit Klein + Selz PC




## Be prepared… *immediately*

**Warn employees to be prepared**

**Areas of improvements, failures, friction and risk**

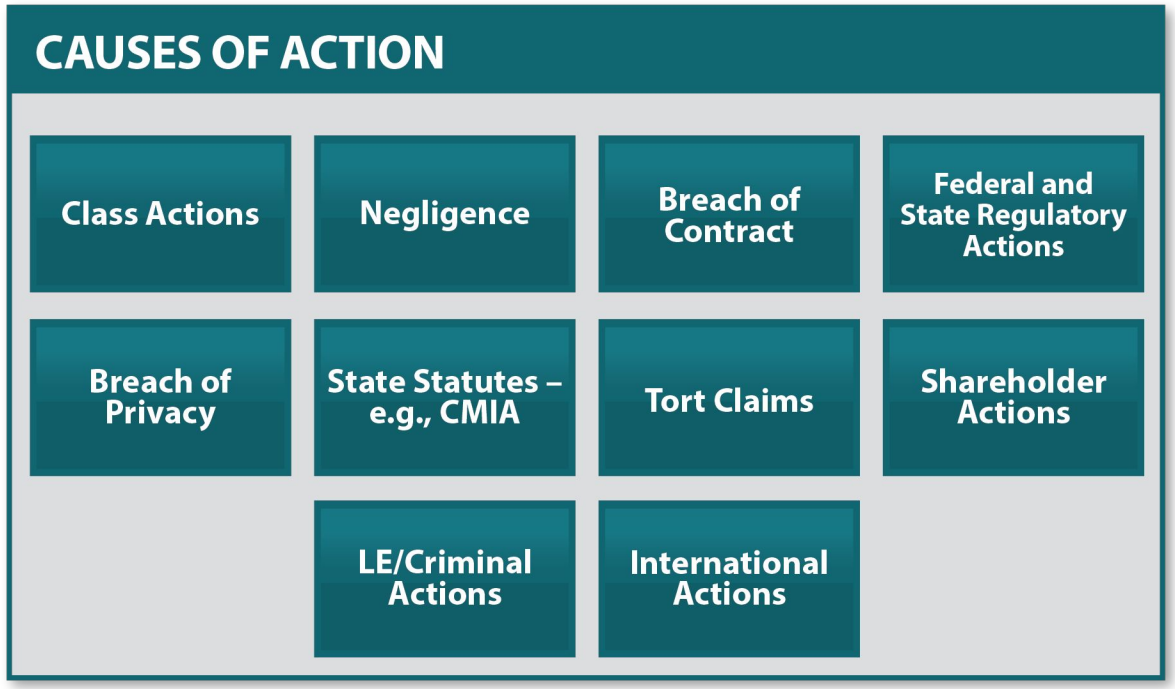
**Areas to reduce remediation time during next breach**

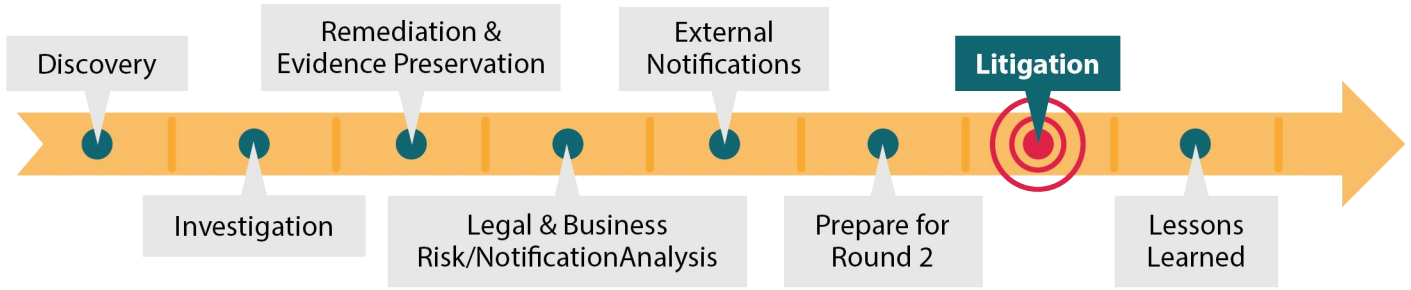
- Technologies
- People - Roles and responsibilities
- Processes - What to do, when to do it, and how to do it … actions by roles and responsibility

**Properly controlled information access**

# Litigation






## 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

Frankfurt Kurnit Klein + Selz PC


**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

Frankfurt Kurnit Klein + Selz PC


**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

Frankfurt Kurnit Klein + Selz PC


**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

Frankfurt Kurnit Klein + Selz PC


**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.





PONDURANCE

# Simplified Recommendation

Frankfurt Kurnit Klein+Selz PC


**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

Frankfurt Kurnit Klein + Selz PC


**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

Frankfurt Kurnit Klein + Selz PC


**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.



PONDURANCE

# Continual Cyber Risk Reduction

Frankfurt Kurnit Klein + Selz PC

| Policy and Control Management | Contextual Management | Threat and IOC Awareness |
|---|---|---|

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

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

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

PONDURANCE

PONDURANCE

Frankfurt Kurnit Klein + Selz PC

# Questions?

# Thank You!

Frankfurt Kurnit Klein + Selz PC

PONDURANCE