NSCP

NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

Incident Response Plan: Remediation and Reporting of a Breach (Intermediate) 9a

Paul Osterberg, CEO & Managing Director, Security Basecamp

Heather Traeger – General Counsel and CCO, Teacher Retirement System of Texas

Norm Ashkenas – Chief Compliance Officer, Robinhood

.

Today's Learning Objectives

1

Understand effective techniques to investigate a breach, develop a strategy for resolution, and document the event.

2

Understand the external resources available during a breach, including law enforcement, third party remediation specialists, cyber liability insurance carrier, and how to manage those resources efficiently and effectively.

3

Develop effective messaging strategies to appropriately escalate an issue internally and externally to avoid compounding an issue.

4

Analyze state and federal regulatory requirements, including reporting obligations.

Overview

Welcome and Framing the Issues

Breach Response Workflow: Investigation & Containment

Managing External Resources Efficiently

Messaging, Disclosure, and Regulatory Reporting

Case Study & Breach Scenario Discussions

NSCP

NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

Welcome and Framing the Issues

Why Breaches Happen—and Why Regulators Care

Overview of Regulation S-P Amendments

Adopt and Implement an Incident Response Program.

Detect, respond, and recover from unauthorized access or use of client information and prevent usage.

Assess, respond and contain the incident, and prevent future unauthorized access / use.

Oversee and monitor service providers.

Adopt and Implement a Vendor Management Program.

Meet Customer Notification Requirements in the Event of a Breach.

Notice required within 30 days of becoming aware of unauthorized access to sensitive customer information, unless an exception is met.

Comply with Enhanced Safeguards and Disposal Requirements.

Maintain Books and Records to Evidence Compliance.

Service Provider Oversight

COMPILE LIST OF KEY VENDORS

ADOPT A POLICY TO GOVERN REVIEWS

ASSIGN RESPONSIBILITIES FOR REVIEWS AND NOTIFICATION / REPORTING

ASSESS VENDOR RISK AND DETERMINE REVIEW FREQUENCY

CONSIDER TERMS TO MANAGE UNRESPONSIVE VENDORS

DOCUMENT VENDOR REVIEWS

REVIEW EXISTING AGREEMENTS FOR NECESSARY CHANGES

ESTABLISH REASONABLE EXPECTATION OF NOTICE WITHIN 72 HOURS OF BECOMING AWARE OF BREACH

The Financial Sector is Under Siege

The cyber threat landscape is rapidly accelerating and diversifying with AI-enhanced attacks. It demands immediate and sophisticated defense strategies to protect financial assets and client trust.

Accelerated Adversary Operations

Shift To Malware-free Attacks

Explosive Social Engineering Growth

GenAI as a Force Multiplier

The Key Attackers

Financial firms face a sophisticated and expanding array of adversaries, from state-sponsored groups to profit-driven cybercriminals, all employing advanced tactics to compromise systems and data.

Nation-State Actors

Ransomware Gangs

Cyber Criminals

Business Email Compromise Actors

High Value Targets

Financial firms are attractive targets due to their PII, funds and reliance on the client trust. Together these make them susceptible to exploitation of both technical vulnerabilities and human relationships.

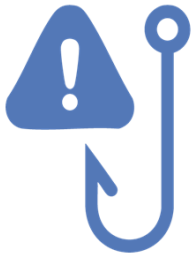
Valuable Data (PII)

Fund Transfer Authority

Exploitation of Trust-Based Relationships

Advisor Impact

Financial Advisor Practices are often impacted in the following ways.



Phishing / Wire Fraud

Ransomware

Lost Laptop

Investing to Reduce or Mitigate Breach Costs

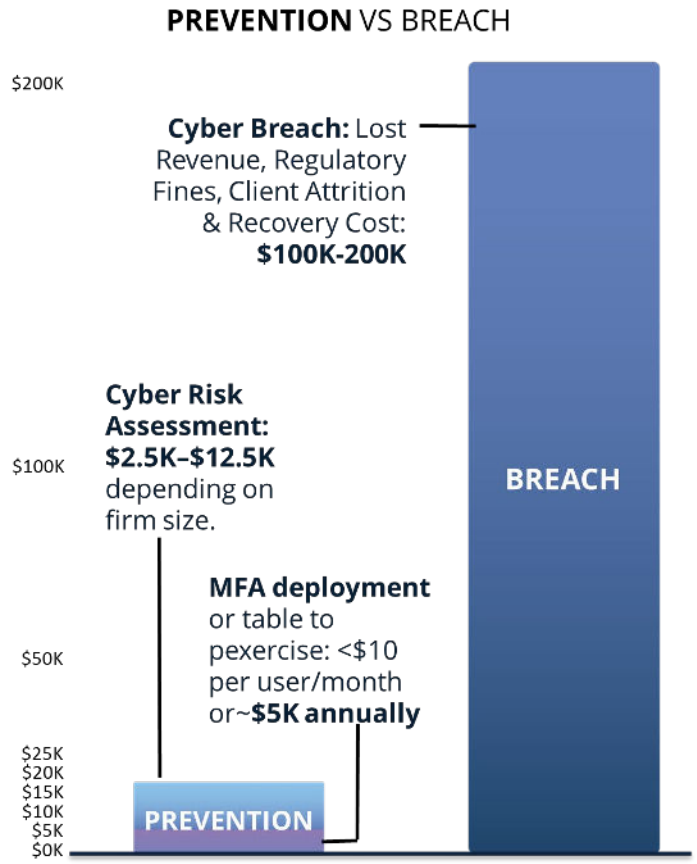
Cost of Breach

TO YOUR PRACTICE

The bad actor's motivation is financial gain. **Investing proactively in preventative measures has an ROI**

- **Lost Revenue**: downtime = missed trades, delayed billing (e.g., $10K–$100K depending on firm size).
- **Regulatory Fines**: SEC/FINRA penalties (hundreds of thousands to millions for failures to disclose or safeguard).
- **Client Attrition**: 30–40% of clients leave after a major breach.
- **Recovery Costs**: IT forensics, insurance deductibles, legal defense.

Source: Security Basecamp Research; Ponemon Institute



NSCP

NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

Breach Response Workflow: Investigation & Containment

From First Alert to Full Containment—Getting It Right the First Time

Threat Intelligence Informs Response Planning

Incident Plan & Remediation:

UNDERSTANDING CYBER THREATS

When an incident occurs, organizations typically move through several phases to identify, contain, and recover from security breaches. Understanding the threat landscape, including who the actors are, their motivations, and their methods, is crucial for effective incident response and remediation.

Informative Breach Resources

The Incident Response Lifecycle

DETECTION & IDENTIFICATION

Alerts from EDR, SIEM, or monitoring tools show anomalies. Also, incidents may be discovered via third-party reports, social media, dark web monitoring, law enforcement, and regulators (e.g., FINRA Threat Intelligence Unit).

CONTAINMENT

Short-term: to isolate affected systems, disable compromised accounts

Long-term: to block attacker persistence, patch exploited vulnerabilities, revoke stolen credentials.

ERADICATE

Removal of malware, backdoors, and unauthorized accounts.

RECOVER

Restore from clean backups and monitor closely for reinfection or further suspicious activity.

LESSONS LEARNED & HARDENING

Post-incident review and improvement of MFA enforcement, credential management, patch cycles, and vendor risk programs.

Who Are the Threat Actors?

From the two reports, there are several categories we might want to look at:

e-Crime Groups

Financially motivated, often ransomware or data extortion operators (e.g., WANDERING SPIDER / Black Basta, CURLY SPIDER)

Nation-states

China: 150% activity surge, focusing on espionage and economic advantage

DPRK (North Korea): currency generation via IT worker infiltration schemes (e.g., FAMOUS CHOLLIMA)

Russia/Iran: disinformation and hybrid operations

Hacktivists

Politically or ideologically motivated disruptions

Insiders / Third parties

Employees, contractors, or partners misusing or exposing access

Why Are They Doing It?

Financial Gain
Ransomware, selling stolen data, or access brokering.

Espionage
Stealing intellectual property or government secrets.

Disruption
Political or ideological motives (hacktivism, election interference).

Dual Motives
Some state actors now "double-dip," mixing espionage with financial crime.

How Are They Doing It? (Part 1)

Credential Abuse & Access Brokers

Most common entry point; valid accounts abused in 35% of cloud breaches

Exploitation of Vulnerabilities

Zero-days in VPNs and edge devices; exploitation linked to 20% of breaches

Social Engineering

Phishing and spear-phishing and even Vishing (voice phishing) up 442% in 2024. There are even some forms of Helpdesk scams (attackers posing as IT).

Source: Verizon Data Breach Investigations Report, 2025

How Are They Doing It? (Part 2)

Interactive Intrusions

79% of detections were malware-free, with attackers using "hands-on-keyboard" RMM tools (e.g., Quick Assist, TeamViewer)

Infostealer Malware

Provides credentials later sold to ransomware operators

Ransomware

Present in 44% of breaches, disproportionately hitting SMBs (88%) .

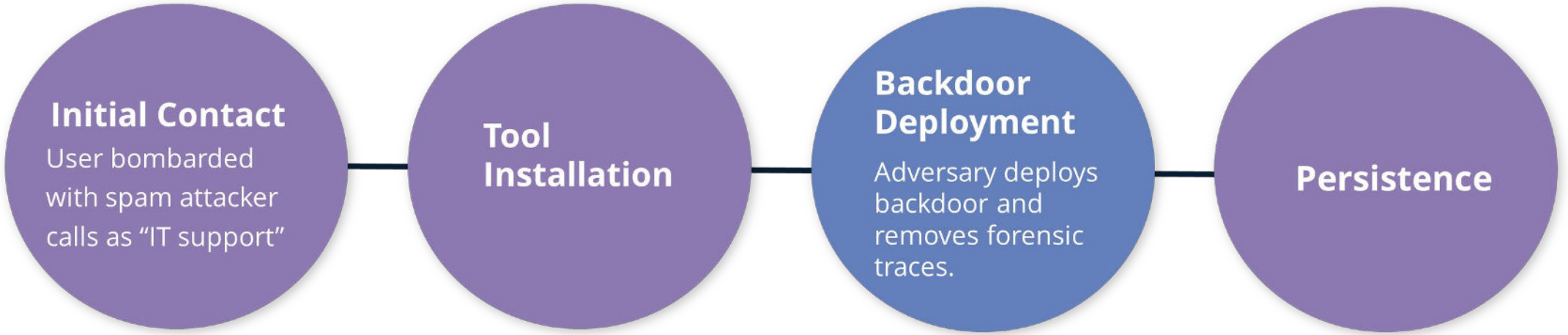
Supply Chain / SaaS Exploitation

Breaches in service providers like Snowflake and Change Healthcare demonstrate systemic risk 【6:16–18†2025 DBIR】

Source: Verizon Data Breach Investigations Report, 2025

What Actually Happens During an Incident*

Example from **CrowdStrike:** CURLYSPIDER social engineering attack.



Building an Incident Response Plan

An IRP drastically reduces the financial and reputational damage of a breach, ensures compliance with regulatory timelines, and preserves business continuity and client trust.

IRP Stages:

Key Roles: CISO, Legal, IT, Communications, Compliance, PR/Communications
Align Plan with **Regulatory Obligations**

Notification Requirements

Communications are Vital to:

- Mitigate financial fallout
- Prevent further harm
- Uphold integrity in the face of a cyber crisis

Understand When to Notify

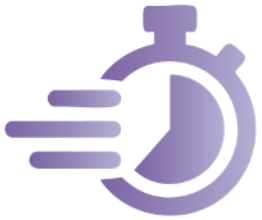
- Employees
- Clients
- Business Partners
- Regulators
- Law Enforcement

Prepare Communication Templates in Advance

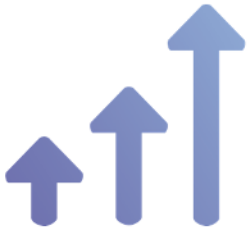
Tabletop Exercise:

Simulate a Phishing-to-Account-Compromise Scenario

Evaluate:



Detection Speed



Internal Escalation

External Communications

Gaps in Procedures

***Include IT, compliance, and executive stakeholders**

NSCP

NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

Managing External Resources Efficiently

Building and Orchestrating Your Outside Response Team

Outsiders are Critical to an Effective Response

Cyber events require specialized expertise and tools – forensics, containment, remediation

Regulators expect documented, timely action (e.g., Reg S-P, FINRA 4530, NYDFS 500.17)

Coordinated external engagement helps **limit business disruption, preserve evidence & privilege,** and **protect brand** and **client trust**

Cyber Insurance: Shield and Guide

Coverage to consider incident response/forensics, legal defense & regulatory fines (where insurable), business interruption & data restoration, ransomware/extortion response

Implications of Using Carrier Resources: insurer panel vendors, policy conditions, pre-approval requirements—know the claims hotline

Action: Map your Incident Response Plan to Policy Terms, Vendor Inventory, Contractual Obligations, and Customer Commitments.

Who You'll Call and When

Outside Counsel – Legal strategy, privilege, regulator liaison (engage as soon as incident confirmed)

Forensic Firm – Determine root cause, scope, and remediation (engaged via counsel)

PR/Communications – Media strategy, customer messaging (when public disclosure likely)

Insurance Carrier – Claims coordination, approved vendors (immediately upon potential claim)

Law Enforcement (FBI/CISA) – Threat intel, possible criminal case (when criminal activity suspected)

PR/Communications & Customer Messaging

Activate the Crisis-Comms Plan Early

Notify internal communications/PR lead as soon as public disclosure is likely. Engage marketing, social, sales, and customer relations teams

Align messaging across internal employees, compliance, IT/security, and executive teams to maintain a single source of truth

Craft Clear, Empathetic Customer Messaging

Explain what happened, what data may be affected, and protective steps (e.g., credit monitoring)

Provide practical resources (hotline, FAQs) and emphasize the firm's remediation actions

Suggested messaging for intermediary partners

Coordinate with Regulators and Legal Counsel

Ensure customer/media statements are consistent with mandatory filings (SEC Reg S-P 30-day, NYDFS 72-hour, FINRA Rule 4530)

Preserve attorney-client privilege by routing drafts through outside counsel

Protecting Legal Position and Evidence

Preserve Attorney–Client Privilege:	Maintain Chain of Custody:	Documentation is Key:
Engage forensics via outside counsel and route communications through legal	Use documented evidence-handling procedures, avoid ad-hoc copying or alterations	Detailed investigation notes and time-stamped decisions support regulatory defense and litigation

Aligning Compliance, Cybersecurity & Executives

Incident Response Lead Convenes a War Room (virtual or physical)

Assign Clear Roles: Internal / External Communication Teams, Compliance/Legal (reporting obligations), IT/Security (technical remediation), Executive (strategic decisions, client relations)

Maintain Single Source of Truth for all Updates; Ensure Internal Incident Communication Channels and Documentation Stores are "Locked Down"

Conduct Daily Briefings until Containment and Notifications Complete

NSCP

NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

Messaging, Disclosure, and Regulatory Reporting

Communicating with Clarity, Compliance, and Confidence

Cybersecurity Regulation & Exam Priorities

SEC Regulation S-P (amended 2024): Customer notice within 30 days; service provider notice within 72 hours; stronger vendor oversight and recordkeeping requirements.

SEC Proposed Rule 10 (Broker-Dealers/SROs) and IA/'40 Act Cyber Rule 206(4)-9: Withdrawn June 12, 2025; any future action would require a new proposal.

NYDFS 23 NYCRR 500 (amended 2023): Notify NYDFS within 72 hours after determining a reportable cybersecurity incident; expanded governance and response expectations.

FINRA Guidance: Ongoing focus on risk-based cybersecurity programs, threat-driven controls, and incident handling (e.g., phishing/BEC, ransomware, vendor breaches).

2025 Examination Priorities

SEC Division of Examinations: Review governance of cyber risk, access controls, data loss prevention, vendor oversight, and Reg S-P readiness.

FINRA: Assess adequacy of incident response handling, customer account protection, and program right-sizing for small firms.

NYDFS: Ensure timely 72-hour reporting, enforce multi-factor authentication, and validate governance certifications and documented remediation plans.

What Good Looks Like – Exam Ready Checklist

- ❑ **Incident Response Program aligned to Reg S-P**: playbooks, customer notice workflow, timestamped awareness determination, and books/records.
- ❑ **Vendor contracts**: include mandatory 72-hour incident notice to your firm and documented monitoring.
- ❑ **Access and DLP controls**: privileged-access reviews, MFA across environments, and outbound monitoring tied to data classification.
- ❑ **Regular tabletop exercises and training** mapped to NIST CSF 2.0 with documented lessons learned.
- ❑ **NYDFS readiness**: criteria for reportable events, portal workflow familiarity, and CISO/Executive annual certification materials.

Overview of Regulation S-P Amendments

Adopt and Implement an Incident Response Program.

Detect, respond, and recover from unauthorized access or use of client information and prevent usage.

Assess, respond and contain the incident, and prevent future unauthorized access / use.

Oversee and monitor service providers.

Adopt and Implement a Vendor Management Program.

Meet Customer Notification Requirements in the Event of a Breach.

Notice required within 30 days of becoming aware of unauthorized access to sensitive customer information, unless an exception is met.

Comply with Enhanced Safeguards and Disposal Requirements.

Maintain Books and Records to Evidence Compliance.

Service Provider Oversight

COMPILE LIST OF KEY VENDORS

ADOPT A POLICY TO GOVERN REVIEWS

ASSIGN RESPONSIBILITIES FOR REVIEWS AND NOTIFICATION / REPORTING

ASSESS VENDOR RISK AND DETERMINE REVIEW FREQUENCY

CONSIDER TERMS TO MANAGE UNRESPONSIVE VENDORS

DOCUMENT VENDOR REVIEWS

REVIEW EXISTING AGREEMENTS FOR NECESSARY CHANGES

ESTABLISH REASONABLE EXPECTATION OF NOTICE WITHIN 72 HOURS OF BECOMING AWARE OF BREACH

Reporting Timelines & Triggers

- **SEC Reg S-P (Amended)** – Notify affected customers within 30 days of becoming aware of unauthorized access unless no-harm exception applies
- **SEC Form 8-K (material incidents)** – File within 4 business days of materiality determination
- **NYDFS 23 NYCRR 500.17** – Report to Superintendent within 72 hours of determining a reportable event
- **FTC GLBA Safeguards Rule** – Customer notice within 30 days
- **State AG Breach Laws** – Most 30–45 days; some as short as 30 days (e.g., CO)
- **Clock starts when you reasonably determine the event is reportable—document that moment**

Internal & External Communication Strategy

- **Internal**
  - Incident Response lead activates GC/CCO, IT, business heads
  - Confirm facts, protect privilege, maintain single source of truth
  - Use pre-approved templates & secure channels
- **External**
  - Regulator filings (SEC, FINRA Rule 4530, NYDFS, other states)
  - Customers: clear, empathetic notices with protective steps
  - Media & investors: consistent, timely updates

- **Internal Preparation Pays:** Pre-draft press/customer/regulator templates and tabletop exercises to test messaging flow

Balancing Transparency & Risk

Transparency Builds Trust

Demonstrates compliance & proactive risk management

Risk Mitigation Limits Exposure

Avoid premature technical details attackers could exploit

Coordinate with counsel to preserve attorney-client privilege

Governance Checkpoints

Legal review before all external statements

Crisis-comms “traffic light”: Green (facts), Yellow (investigating), Red (speculative—omit)

PR/Communications & Customer Messaging

Control the Narrative

Designate a single spokesperson and approved talking points

Time public statements to follow regulatory notifications to avoid surprises

Engage Media Proactively but Carefully

Monitor traditional and social media for misinformation

Respond rapidly with accurate updates to protect reputation

Document All Communications

Retain scripts, emails, press releases, and social media posts for regulatory review and potential litigation defense

Mandatory vs. Voluntary Disclosures

- **Mandatory**
  - SEC Reg S-P 30-day customer notice
  - SEC Form 8-K (material)
  - NYDFS 72-hr reporting
  - FINRA Rule 4530 event reports
- **Voluntary / Strategic**
  - FS-ISAC or industry threat sharing
  - Proactive client outreach beyond statutory requirement
  - Public statements to reassure market
  - Coordinated disclosures to partners/vendors

- **Tip:** When voluntarily sharing, align with counsel to avoid creating new liability.

NSCP

NATIONAL SOCIETY OF COMPLIANCE PROFESSIONALS

Case Study & Breach Scenario Discussions

Lessons from the Front Lines—What Worked, What Didn't

Evolving Breach Threats

- **Deepfake & AI-Driven Impersonation**: Realistic audio/video used to spoof executives and authorize fraudulent wire transfers or leak sensitive data.
- **Generative AI Attacks**: Automated phishing, malware creation, and social engineering campaigns at unprecedented scale and speed.
- **Malicious Remote Workers**: State-sponsored actors (e.g., North Korea) infiltrating firms as employees or contractors to steal data or gain network access.
- **Synthetic Identities & Credential Abuse**: AI-created identities and stolen credentials enable stealthy account compromise and lateral movement.
- **Evolving Regulatory Scrutiny**: SEC, FINRA, and NYDFS emphasize incident-response readiness for AI-enabled threats and third-party workforce risks.
- **Defensive Priorities**: Strengthen identity verification (voice/biometric), vendor/employee vetting, continuous network monitoring, and staff training on emerging attack vectors.

Case Study: SolarWinds

Background: In 2020, attackers compromised SolarWinds' Orion software updates, impacting thousands of government agencies and private organizations worldwide.

The compromise remained undetected for many months, allowing attackers to infiltrate sensitive networks and exfiltrate data.

What Didn't Go Well

Delayed Detection:

Malicious code inserted into Orion updates was active for ~9 months before discovery.

Insufficient Code-Signing & Supply Chain Security:

Attackers successfully altered signed software without triggering alerts.

Inadequate Patching & Decommissioning Processes:

Led to devices and systems that were able to be compromised

Limited Internal Segmentation:

Once inside, attackers moved laterally across customer networks with limited detection.

Communication Gaps:

Early public messaging was criticized for lack of detail and timeliness, creating confusion among customers and regulators.

Vendor Oversight Weakness:

Customers relied heavily on SolarWinds' assurances without additional monitoring or verification.

Regulatory & Legal Fallout:

Multiple investigations, lawsuits, and reputational damage underscored governance and compliance gaps.

Key Lessons for Financial Services Firms

Strengthen	Strengthen **software supply-chain risk management** and **require verifiable vendor security attestations.**
Implement	Implement **rigorous code-signing verification** and **continuous monitoring of third-party updates**.
Segment	Segment **internal networks** to limit lateral attacker movement and **enhance detection capabilities.**
Maintain	Maintain a **pre-approved crisis-communication plan** to ensure timely, accurate external messaging to clients and regulators.
Include	Include **supply-chain compromise scenarios** in **tabletop exercises** and **incident response playbooks**.

Best Practices

IMMEDIATE CONTAINMENT AND EVIDENCE PRESERVATION

EARLY ENGAGEMENT OF OUTSIDE COUNSEL AND FORENSICS TO PRESERVE PRIVILEGE

CLEAR, CONSISTENT COMMUNICATION WITH EMPLOYEES, STAKEHOLDERS AND REGULATORS

DOCUMENTATION OF ALL ACTIONS AND DECISIONS FOR AUDIT AND COMPLIANCE

Best Practices – SEC and FINRA Focus

Document	Preserve	Maintain	Ensure	Retain
Document "awareness" timing and decisions to support SEC Reg S-P's 30-day notice trigger and FINRA Rule 4530's incident reporting clock.	Preserve attorney–client privilege by routing forensic and investigative work through outside counsel.	Service-provider oversight: maintain contracts requiring 72-hour incident notice and evidence of controls (aligning with Reg S-P amendments and NYDFS 23 NYCRR 500).	Board/Executive briefings: ensure cyber incidents and response lessons are formally communicated to governing bodies to demonstrate governance oversight.	Comprehensive recordkeeping: retain IR playbooks, tabletop reports, and post-mortems for examination and enforcement reviews.

Not-So-Good Practices

DELAYING INTERNAL ESCALATION OR UNDERESTIMATING INCIDENT SEVERITY

COMMUNICATING PREMATURELY OR WITHOUT LEGAL REVIEW

FAILING TO MEET STATUTORY NOTIFICATION TIMELINES (E.G., NYDFS 72-HOUR RULE)

INSUFFICIENT DOCUMENTATION OF ACTIONS TAKEN OR LESSONS LEARNED

Not-So-Good Practices – SEC & FINRA Pitfalls

Failure to meet the Reg S-P 30-day customer notice or to **conduct a "reasonable investigation"** before deciding not to notify.

Incomplete or delayed FINRA Rule 4530 filings, or **lack of 30-day follow-up** after a significant cyber event.

Inadequate vendor management, such as no evidence of due diligence or lack of contractually required breach notification.

Missing documentation of key actions and timing, making it impossible to prove compliance during an SEC or FINRA exam. Improvised media/PR response that contradicts regulatory filings or creates reputational and enforcement exposure.