

Cybersecurity Demystified

PRACTICAL GUIDANCE FOR TODAY'S FINANCIAL FIRM



www.securitybasecamp.com
(949) 330-0899
paul@securitybasecamp.com

Overview



Detect & Mitigate Cybersecurity Risks

Be Secure. Be Compliant.

Security Basecamp (SBC) has highly experienced business-oriented cybersecurity professionals combining expertise across the breadth of regulations, security frameworks, and information technology environments.

[ABOUT US](#)

[vCISO](#)

[Risk Assessments](#)

[Vendor Due Diligence](#)

[Penetration Testing](#)



Security Basecamp: Core Team

Exceptionally deep cybersecurity expertise



Paul Osterberg

- CEO
- 20,000+ hours cybersecurity experience
- vCISO for 10+ Years (Wall Street, IBDs, RIAs)



Leslie Ko

- Senior Security Architect
- Network / Cloud Expertise
- Automation via Artificial Intelligence



Patrick Carra, CISSP

- Cybersecurity Researcher and Architect
- Instructor
- 10+ Cyber Credentials



Marie Larouche

- Cyber Program / Project Management
- HR / Recruiter



Samantha Viksnins, CPA

- Cyber Program / Project Management
- SOC2 Controls



Pamela Kirui

- PhD Candidate, Digital and Cyber Forensics
- Artificial Intelligence / Deep Fake Analysis

The ABCs of Cybersecurity



Advisor Toolkits

These 5 Security Basecamp toolkits provide support you need to start your firm's cybersecurity focus today.



Home & Remote Work Guide - Secure your laptop, router, and phone

Client Cyber Security Guide - How to keep clients from wiring money to fraudsters

Securing Your Business - Practical steps to secure the branch office

Mobile Security Best Practices - Protect your smartphone from AI deep fake and phishing

Incident Management Guide - Know your 30-day and 4-day SEC deadlines

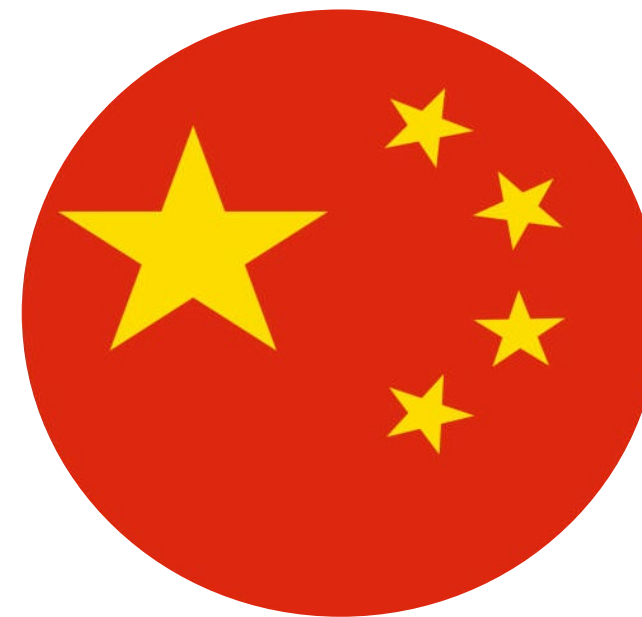
<https://www.securitybasecamp.com/insights-events/#upcomingEvents>

The Great Cyber Schism

The internet is splitting into two competing models, forcing businesses to confront fundamentally different approaches to cybersecurity, AI, and innovation.



The Open Camp:
U.S., Europe, Allies



The Closed Camp:
China, Russia, Iran, North Korea

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

Notable U.S. Breaches / Intrusions

Attributed to China

Name / Incident	Approximate Scale / Impact	Description / Notes
Equifax breach (2017)	~145 million U.S. consumers affected	Stolen personal data (SSNs, birthdates, addresses, etc.).
OPM (Office of Personnel Management) breach (2014–2015)	~22 million personnel records	Included sensitive background investigation data, fingerprint data, etc.
2024 U.S. telecommunications / telecom network hack (“Salt Typhoon”)	Over 1 million call records / metadata; multiple telecom providers	The hackers reportedly accessed court-ordered wiretap systems, phone metadata of U.S. users (including gov’t / political figures), and deeply penetrated telecom infrastructure
U.S. Treasury / BeyondTrust compromise (2024)	Stolen credentials / remote-access vector; access to unclassified documents	Attackers compromised third-party remote-management software (BeyondTrust) and used it to access Treasury workstations.

How are They Doing It?



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 or Corporate Executives).

Source: Verizon Data Breach Investigations Report, 2025

How are They Doing It?



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%) .



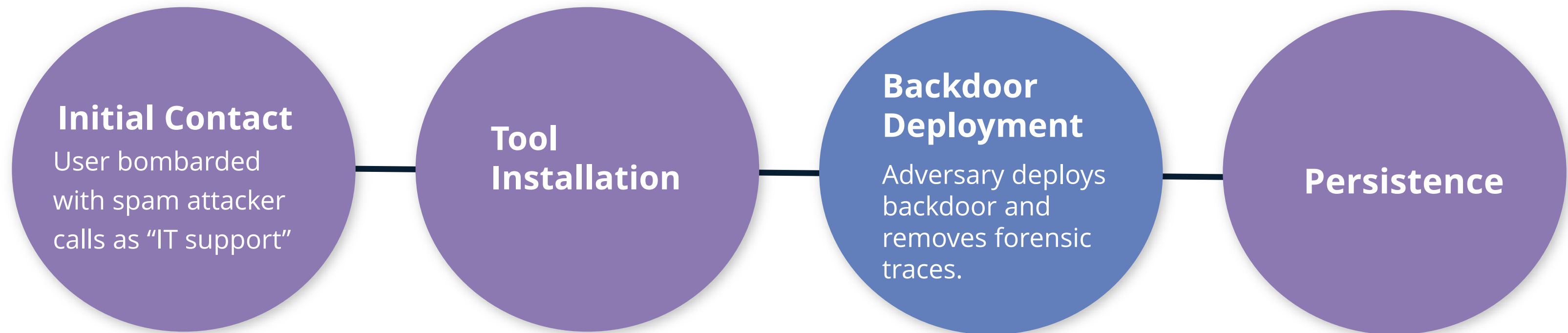
Supply Chain / SaaS Exploitation

Breaches in service providers like Snowflake and Change Healthcare demonstrate systemic risk.

Source: Verizon Data Breach Investigations Report, 2025

What Happens During an Breach

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



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.



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

Advisory Impact

Financial Advisor Practices are often impacted in the following ways.



Phishing / Wire Fraud



Ransomware



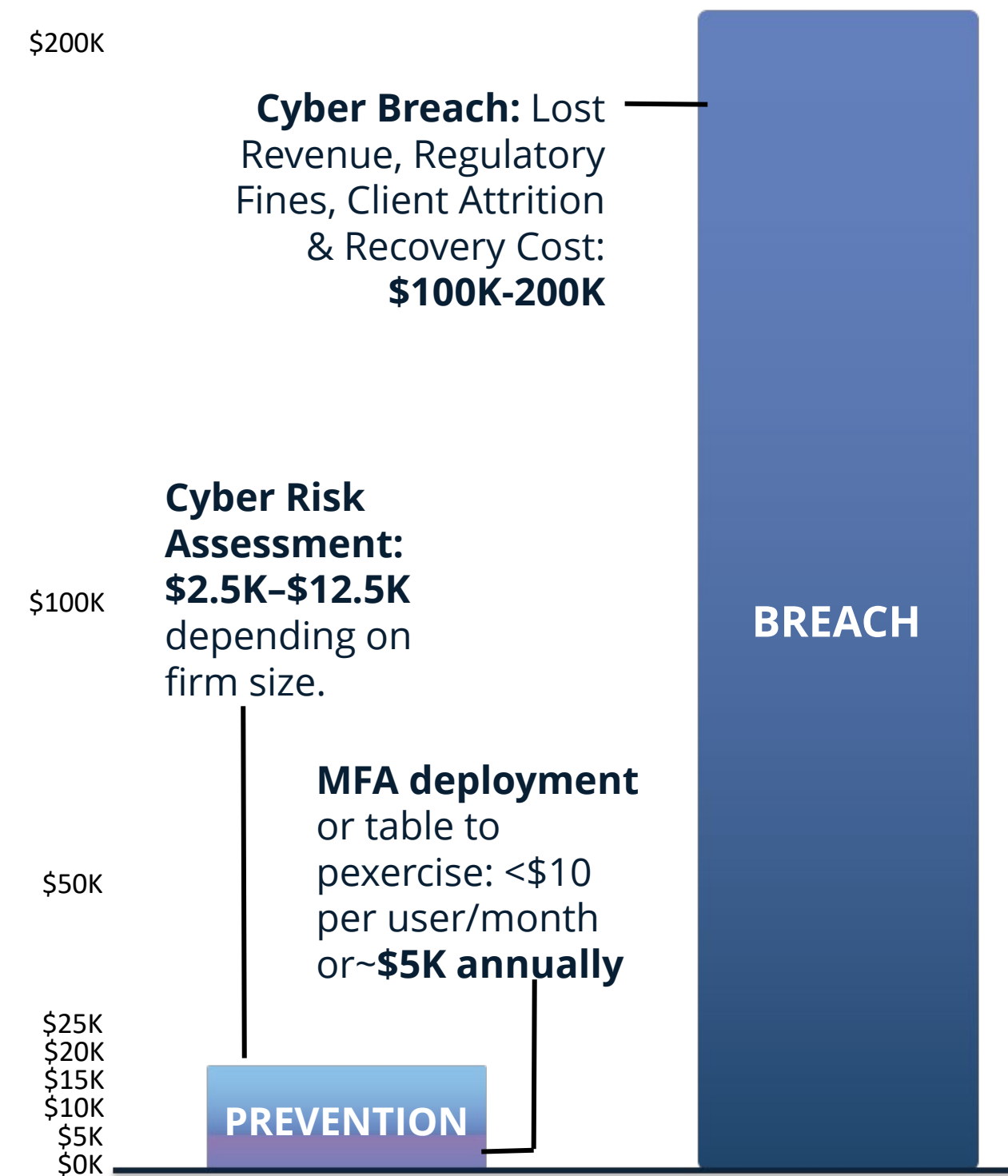
Lost Laptop

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.

PREVENTION VS BREACH



Regulatory Compliance

Such incidents demonstrate why SEC, FINRA, and NYDFS mandates are vital blueprints for protecting financial stability and investor confidence.



SEC: Reg. S-P



FINRA: Rules



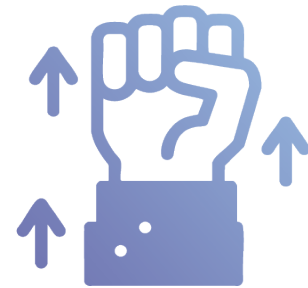
NYDFS: 23 NYCRR
Part 500

The Path to Compliance

Beyond compliance, proactive cybersecurity builds client trust, safeguards your firm's business continuity, and transforms risk into a strategic advantage.



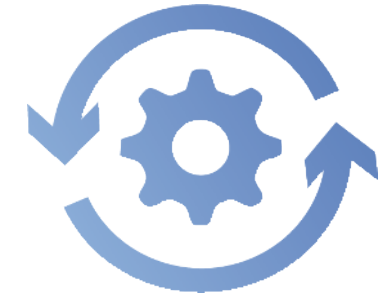
Proactive Risk
Assessment



Strengthen Controls
and Training

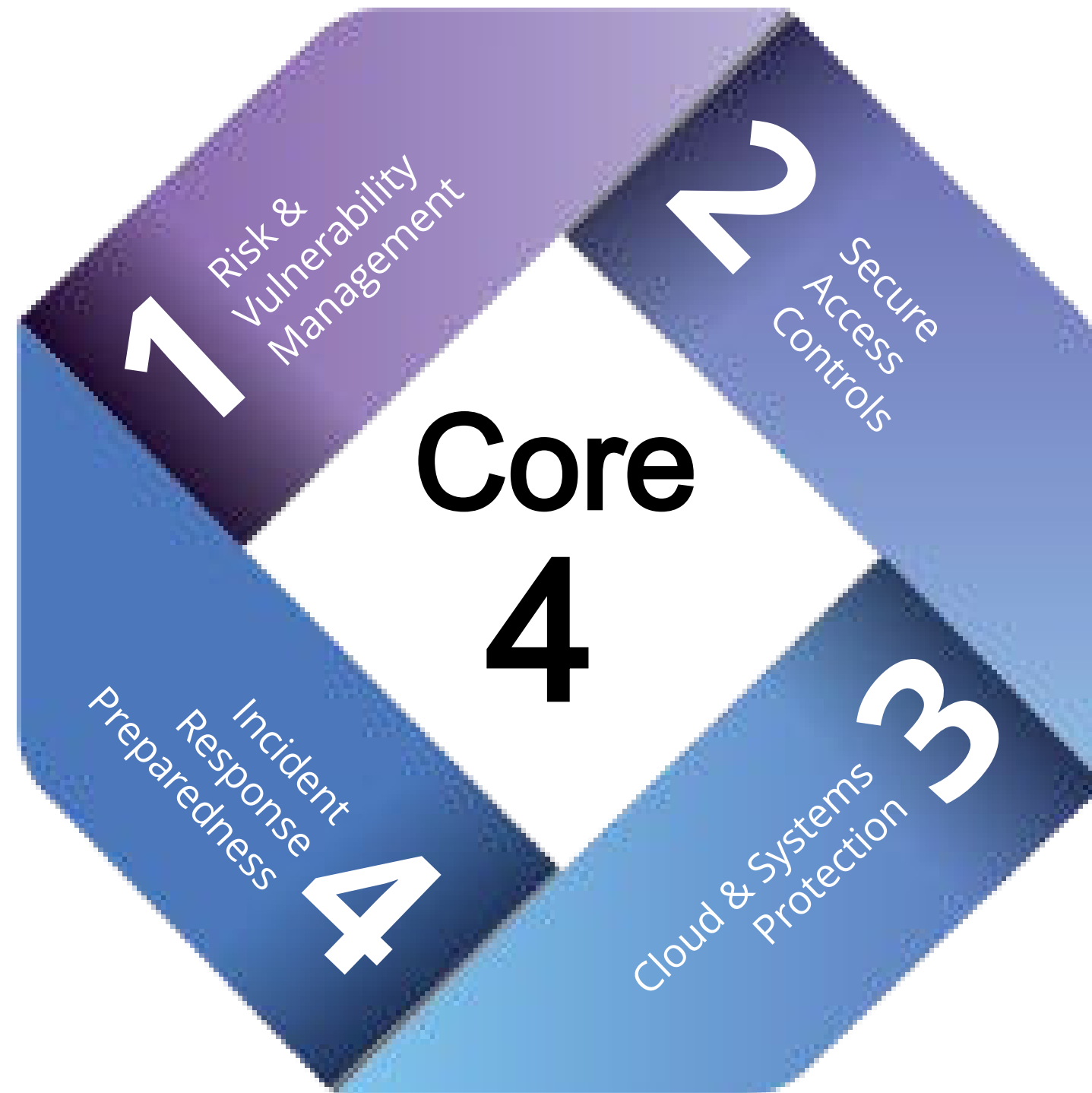


Preparedness and
Response



Adaptive
Compliance

Getting Secure



Robust cybersecurity across these four essential domains directly safeguards your financial assets, ensures regulatory compliance, and protects long-term business resilience.

Advisor Toolkits

These 5 Security Basecamp toolkits provide support you need to start your firm's cybersecurity focus today.



Home & Remote Work Guide - Secure your laptop, router, and phone

Client Cyber Security Guide - How to keep clients from wiring money to fraudsters

Securing Your Business - Practical steps to secure the branch office

Mobile Security Best Practices - Protect your smartphone from AI deep fake and phishing

Incident Management Guide - Know your 30-day and 4-day SEC deadlines

<https://www.securitybasecamp.com/insights-events/#upcomingEvents>



3 Things to Do Now in Your Practice

DEFENDING YOUR PRACTICE IS EASIER THAN YOU THINK.

Monitor: Microsoft Defender, AWS CloudTrail, AWS Guard Duty



Turn on MFA everywhere

(custodians, email, CRM, trading platforms).

Run a Cybersecurity Risk Assessment

(baseline vulnerabilities, vendor risk, gaps vs SEC/FINRA expectations).



Test Your Incident Response Plan

(simulate phishing → account takeover, make sure escalation & communication work).

Risk & Vulnerability Management



Cyber Security

RISK ASSESSMENT

Make performing annual risk assessments (or more frequently if the business/threat landscape changes) a business imperative.



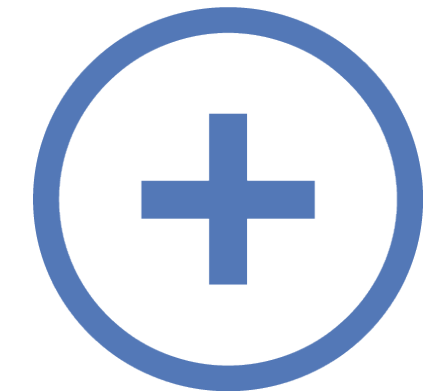
Critical Assets



Regulatory Obligations



Threats & Vulnerabilities



Mitigating Controls

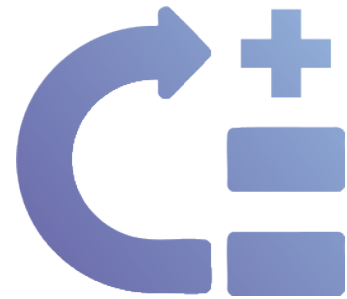
Reference Frameworks: NIST CSF, CIS Controls, SEC Reg. S-P

Vulnerability Management

Know what you protect through a robust asset inventory and act swiftly on critical vulnerabilities (within 30 days) to minimize attack surface, reduce breach likelihood, and directly safeguard operations and reputation.



Automated Scanning



CVSS scores + Context =
Prioritize Remediation



Timely Patching



Maintain Asset Inventory

Secure Access Controls



Multi -Factor Authentication (MFA)

Implement MFA, especially app-based or hardware tokens, as your front-line defense against credential theft and account takeovers, directly protecting client assets, sensitive data, and maintaining the invaluable trust essential to our financial firms.



Email



CRMs



Custodian & Trading
Platforms



Remote Access
(VPN, RDP)

***App-Based MFA/Hardware Tokens**

Account Management

Audit accounts and implement role-based access control to eliminate unnecessary access points, fortify defenses against compromise, and control access to financial and client data.

Principle of Least Privilege:



Audit & Remove Stale or Unused Accounts



Role-Based Access Control (RBAC)



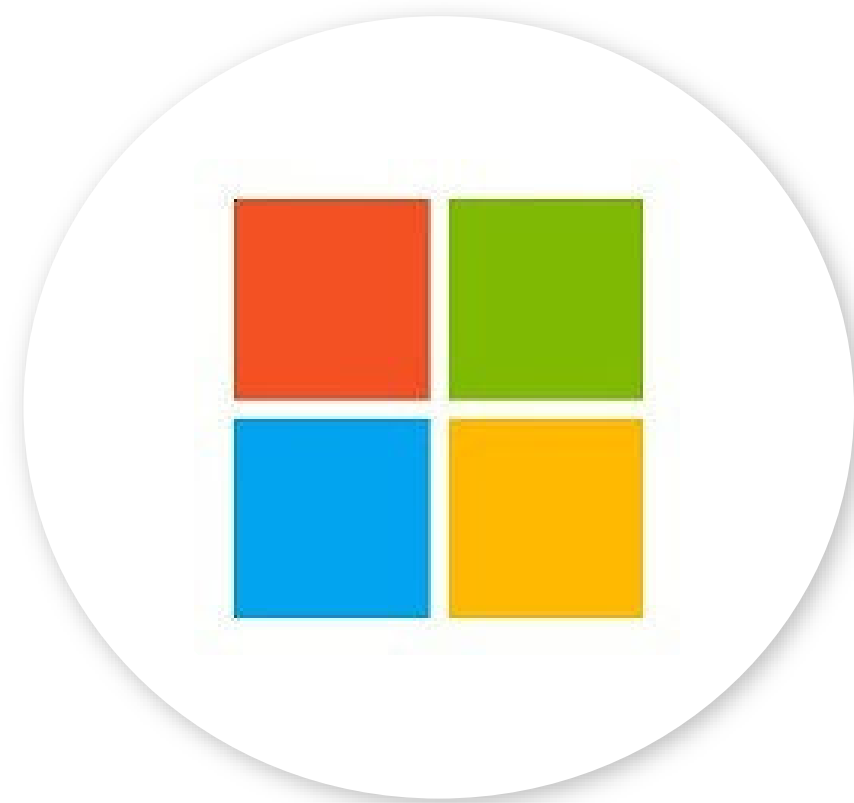
Restrict Administrative Privileges



Monitor Account Usage

Protect, Cloud & Systems





Microsoft 365,
Azure, AWS

Secure Cloud Platforms

Harden cloud configurations and implement monitoring to preempt misconfigurations, detect anomalies, and reduce the financial and reputational impact of cloud-based attacks.

HARDEN CONFIGURATIONS:

- **Enable Auditing and Logging**
- **Disable Legacy Protocols (IMAP, POP3)**
- **Use Conditional Access Policies**

Monitor: Microsoft Defender, AWS CloudTrail, AWS GuardDuty



Data Encryption

STORAGE HYGIENE

Data encryption and storage hygiene are vital investments. They ensure the confidentiality and integrity of client records, secure your firm's reputation, mitigate financial liabilities, and strengthen your competitive position.

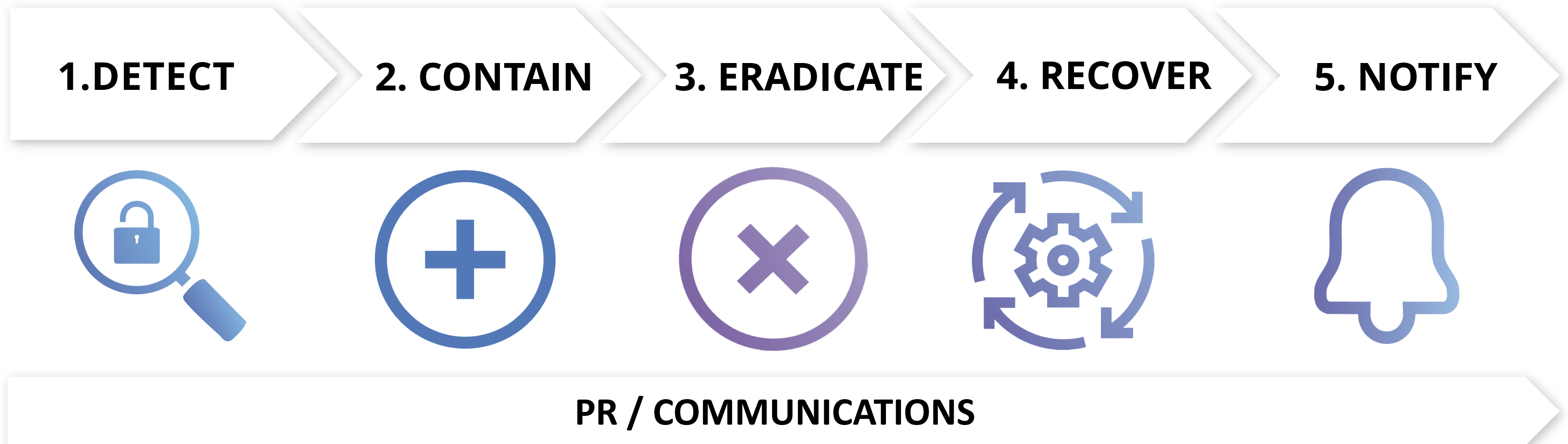
- **Encrypt Data at Rest and In Transit** (AES-256, TLS 1.2+)
- **Use DLP** (Data Loss Prevention)
- **Segment Client Data by Advisor/Team** (Confidentiality)

Incident Response Preparedness



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.

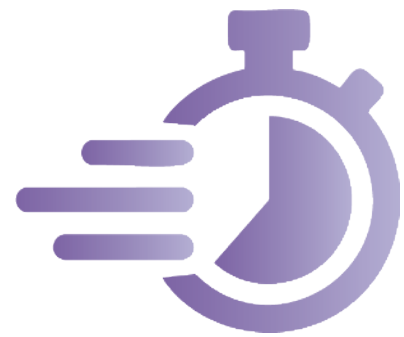


Key Roles: CISO, Legal, IT, Communications, Compliance, PR/Communications
Align Plan with **Regulatory Obligations**

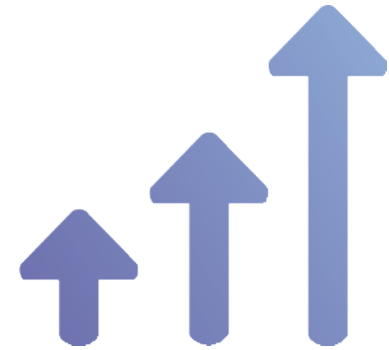
Tabletop Exercise

Simulate a Phishing-to-Account-Compromise Scenario

Evaluate:



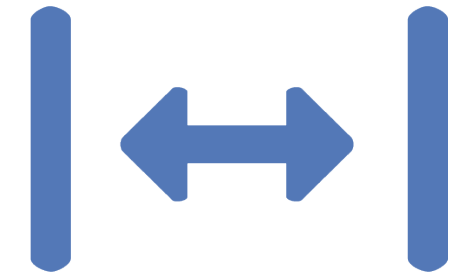
Detection Speed



Internal Escalation



External Communications



Gaps in Procedures

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

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.



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

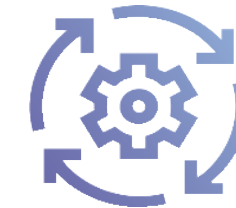
Short-term: to isolate affected systems, disable compromised accounts

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.

Case Studies



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.

SolarWinds: 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.

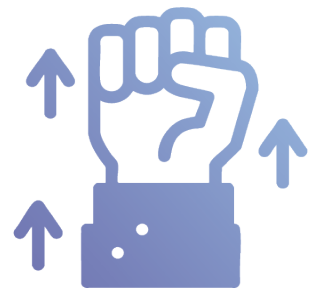
Regulatory & Legal Fallout:

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

Summary & Next Steps



Recap



Strong Access
Management



Proactive Risk
Identification/Patching



Secure Cloud Posture and
Data Handling



Tested/Updated IR Plan
Take Backups

Next Steps

- Perform a Risk Assessment
- Consider External Validation
- Security Basecamp Can Help You Do This!



Why You Should Be Bullish

Despite the rising threats, U.S. businesses and entrepreneurs are well-positioned to lead in a digital world — if they take cybersecurity seriously and view it as a competitive advantage.

1

Most Innovative/
Trusted Firms and
Infrastructure;
Culture of Resilience
and Reinvention

2

Reward Strong
Security, Punish
Negligence

3

Leverage Open-Source
Intelligence,
Collaborative Defense,
and Public-Private
Innovation





The SEC

The SEC's updates to Reg. S-P demand robust cyber risk management, with an emphasis on timely, material incident disclosure and board accountability.

- **Timely Disclosure** (Form 8-K)
- **Incident Response Plans** (Reg. S-P Amendment)
- **3rd-Party Vendors** (Reg. S-P Amendment)



FINRA

Expects a tailored, risk-based cybersecurity program focused on safeguarding customer data and ensuring firm resilience.

- **Business Continuity Plans (Rule 4370):** Firms are required to create and maintain BCPs to ensure operational continuity.
- **Strong Controls (Rule 3120):** Firms must test their supervisory control systems and procedures.
- **Reporting Requirements (Rule 4530):** Firms must report certain events such as cybersecurity incidents.



NYDFS

Expects a tailored, risk-based cybersecurity program focused on safeguarding customer data and ensuring firm resilience.

- **Designated CISO** and Formal Program (500.2, 500.4)
- **Rigorous Testing** (500.5, 500.8)
- **Strong Authentication** (500.12)
- **Strict Reporting** (500.17)
- **Awareness Trainings** (500.14)