GUIDE

Cyber Compliance Is a Necessity in the Digital World — Are You Prepared for Cyber Risks?

Why Smarsh Cyber Compliance is the shield your firm needs

smarsh®

Introduction

In today's modern world, where nearly every organization conducts business digitally, cyberattacks have grown more frequent and severe. According to the IBM Cost of a Data Breach Report, the average cost per breach in 2023 was a staggering $4.45 million. The costs of these breaches have significantly increased in the last few years and are predicted to continue to accelerate in the years ahead.

Regulatory bodies have taken decisive action to bolster cyber compliance measures in response to these escalating risks. The U.S. Securities and Exchange Commission (SEC) proposed cyber security reforms in the investment management industry and new requirements to address cybersecurity risks to the U.S. Securities Markets.

Every organization and its stakeholders are vulnerable to cyber intrusions, which can have repercussions that extend beyond financial losses. New regulations are being reviewed, and as organizations navigate this complex and evolving landscape, the need for strong cyber compliance solutions becomes increasingly apparent. By adopting cyber compliance measures, organizations can fortify their defenses, reduce risks, and create a secure environment that supports sustainable growth and success before the proposed rules are finalized and enforced.

This guide delves into how regulators address cyber risks and what organizations can do to ensure they are prepared – without unnecessary headaches.

How the SEC is addressing cyber risk and why it matters

The increased reliance on information systems has correspondingly increased cybersecurity risks, and the tactics used to compromise these systems have grown more sophisticated. The interconnectedness of these systems has further allowed threat actors to exploit vulnerabilities in these systems, which can have a cascading effect from one entity to another.

The SEC has proposed rules designed to address and mitigate cybersecurity risk by requiring Market Entities to take measures to protect themselves and investors from the harmful impacts of cybersecurity incidents.

Proposed Rule 10: What to know

The SEC has proposed a new rule, form, and amendments to existing recordkeeping rules. The proposal requires market entities to address cybersecurity risks through policies and procedures. It also mandates immediate notification to the SEC of a significant cybersecurity incident. Additionally, it involves reporting detailed information to the SEC about such an incident and making public disclosures to improve transparency regarding cybersecurity risks and significant cybersecurity incidents.

Potential implications for other regulations

It's important to be aware that the adoption of Rule 10, as proposed, may also affect market entities subject to Regulation SCI, Regulation S-P, Regulation ATS, and Regulation S-ID. Should Rule 10 be adopted, market entities will need to review the applicable regulations and stay informed about proposed amendments to existing regulations

Cybersecurity risk management policies and procedures

Proposed Rule 10 would require all market entities to establish, maintain, and enforce written policies and procedures that are reasonably designed to address their cybersecurity risks. The SEC framework for policies and procedures primarily relies on the NIST Framework and CISA Cyber Essentials Starter Kit. The Proposed Rule 10 indicated that market entities engaged in business activities regarding crypto assets are exposed to heightened cybersecurity risks. These entities may want to include additional measures tailored to these business activities.

READ THE BLOG

Cybersecurity Risk Management:
The Implications of Proposed SEC Rule 10

Organizations need both cybersecurity and cyber compliance

Cybersecurity isn't new. However, many firms may be unconsciously looping cyber compliance in with cybersecurity.

Many people understandably think these are interchangeable terms and mean the same thing. However, cybersecurity and cyber compliance are distinctly different and describe different — but equally important — concepts.

Cyber compliance

Cyber compliance describes the aligning of cybersecurity systems to regulatory agency requirements. However, one of the biggest mistakes firms make is treating cyber compliance as solely a cybersecurity — or IT — issue. The role of cyber compliance is to protect an organization through a regulatory lens by reviewing policies and procedures against gaps, ensuring proper recordkeeping, completing and filing appropriate disclosures, and reporting significant incidents.

Cybersecurity

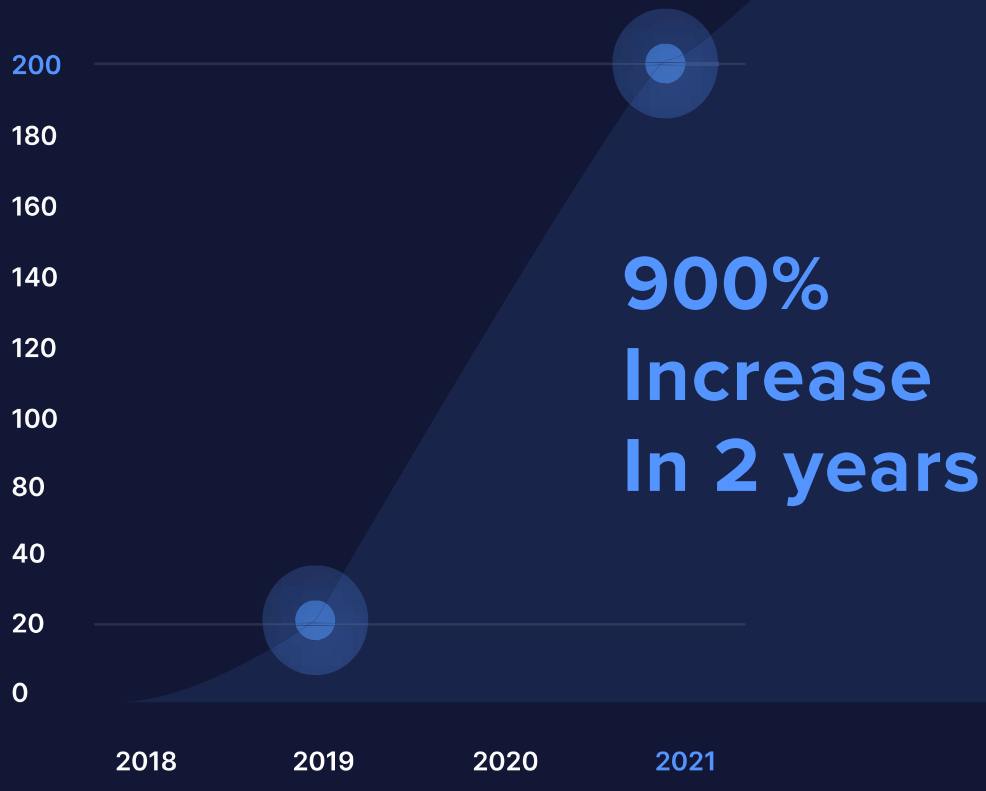
Cybersecurity can be thought of as the controls that protect an organization's IT infrastructure. This includes end-user devices, networks, cloud assets, applications and their business and customer data. Cybersecurity largely falls under four key pillars; strategy, technology, management, and training and communication.

With regulators heavily involved, organizations need to determine accountability, who will be the face of cyber compliance and vendor risk management for regulators — and the "what" and "how" to implement processes and procedures, including how this can all be executed without additional resources and time.

It’s not about best practices anymore — these are requirements

In today’s business landscape, cybersecurity is no longer just a matter of best practices; it has become a regulatory requirement. With the increasing focus from regulatory bodies, organizations are now obligated to enhance their cyber posture to meet these stringent requirements.

In 2019, the FINRA Cybersecurity Specialist team handled approximately 20 cyberattacks. In 2021, there were 200[1]. That’s a 900% increase and it’s only continued to grow. The 2023 Verizon DBIR report found there were 1,832 cyber incidents — 480 within the financial and insurance sectors.



These numbers are not meant to cause fear. However, they are a call to action. There are times to wait and see and there are times to be proactive — we’re living in the latter scenario when it comes to cybersecurity and cyber compliance. Even though enforcement is not happening yet, firms have already begun receiving audit requests. Firms should take that as a sign to prepare for near-future enforcement.

1. FINRA Cybersecurity Specialist Team - 2022 FINRA Cybersecurity Conference

Smarsh makes cyber compliance easy — today and in the future

Modern organizations need a comprehensive approach to cyber compliance that enables continuous monitoring of cybersecurity risks from a single vendor. The Smarsh Cyber Compliance platform provides a unique, holistic cyber risk score for devices, networks, and users, allowing you to identify and address cybersecurity gaps effectively.

The Smarsh Cyber Compliance platform offers a powerful, all-encompassing approach to cyber compliance from a single vendor, covering endpoint cyber posture monitoring and remediation for devices, phishing training, security awareness, compliance behavior assessments for users, continuous network vulnerability scanning and reporting, and comprehensive vendor due diligence including 3rd party risk data and OFAC sanctioning reports.

Key benefits:

Comprehensive monitoring: Easily monitor users, devices, vendors, and networks with an easy-to-install, lightweight active monitoring application that runs on various devices.

Auto remediation: Save time and reduce risk with built-in remediation applications that automatically fix issues in real-time, including remote desktop, auto VPN, data leakage monitoring, password policy enforcement, anti-virus/anti-malware status checks, and device encryption.

Simple UI and dashboard: Use a single-pane-of-glass solution to access a comprehensive dashboard with a cyber risk score and granular analytics features for gaining valuable insights from your data.

Alerts, reports and policies: Stay ahead of risk with regulatory reports, event logs, and alerts. Compliance teams can establish policies, conduct virtual audits, and push remediation services to devices when malicious behavior is detected.

Add-on security services: The Cyber Compliance platform offers a full suite of additional security services that seamlessly integrate into the platform, including compliance-based reporting, risk-based authentication, credential theft monitoring, and security awareness and phishing training.

By leveraging the Smarsh Cyber Compliance platform, organizations can ensure the highest level of organizational security while reinforcing compliance initiatives. Don't hesitate to start a conversation with one of our experts today to secure your organization with the Smarsh Cyber Compliance platform.

smarsh®

Smarsh enables companies to transform oversight into foresight by surfacing business-critical signals in more than 100 digital communications channels. Regulated organizations of all sizes rely upon the Smarsh portfolio of cloud-native digital communications capture, retention and oversight solutions to help them identify regulatory and reputational risks within their communications data before those risks become fines or headlines.

Smarsh serves a global client base spanning the top banks in North America, Europe and Asia, along with leading brokerage firms, insurers, and registered investment advisors and U.S. state and local government agencies. To discover more about the future of communications capture, archiving and oversight, visit www.smarsh.com.

Guide - 10/24

1-866-762-7741 www.smarsh.com @SmarshInc SmarshInc Company/smarsh