Cybersecurity vs. Cyber Compliance:
The Compliance Professional's Guide

Introduction

Cybersecurity isn't new — it's been a major concern and frequent topic of discussion in the financial services industry for decades. In more recent years, a different but related area is gaining regulatory attention: cyber compliance.

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.

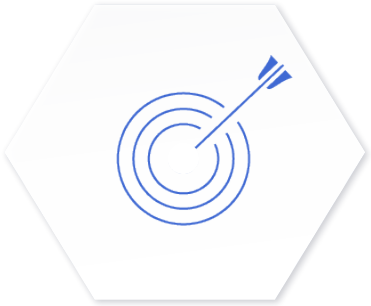
In this guide, you'll learn how to:

- Differentiate these terms and how they relate to compliance accountabilities
- Demonstrate to regulatory bodies that you have a proactive, continuous program in place
- Achieve and establish a robust risk posture by using automated compliance technologies

Cybersecurity

Most firms understand cybersecurity as the controls that are in place to protect their IT infrastructure. This includes end-user devices, networks, cloud assets, applications and their business and customer data.

Cybersecurity has traditionally been a risk that falls under the purview of IT and encompasses the gamut of accountability from infrastructure to employee training. While this is a complex topic, cybersecurity largely falls under four key pillars:



Strategy

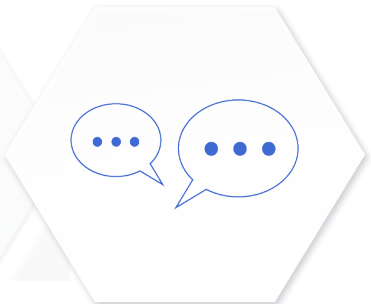
The overall approach to the cybersecurity issue and how it aligns to the needs of the business and clients

Technology

The identification and implementation of tools required to meet strategy objectives

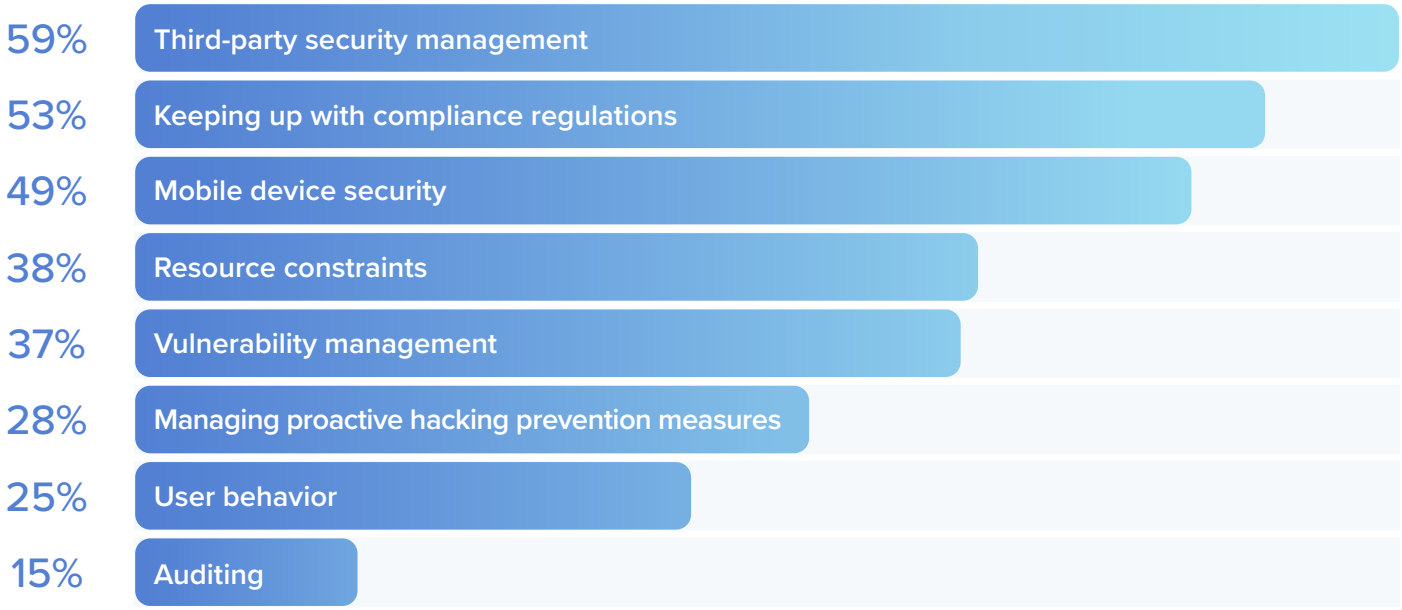
Management

The process to ensure security systems are maintained, up to date, and responsive to incidents



Training & Communication

The continuous process of training employees to recognize and communicate threats and attacks



1 Source: Salesforce Top Data Security Trends for 2022 - a survey of 300 North American IT leaders across both regulated and nonregulated industries

Cybersecurity is more than securing your firm's internal data

Establishing these cybersecurity pillars will enable firms to address changes and trends caused by the evolving technology landscape. Already, most firms have cybersecurity policies in place to support hybrid and work-from-anywhere models.

More than ever, firms are turning to partner vendors or third-party applications to maximize the value of their data. And having more access points means having more cyber risks.

Vendor risk management is an important part of a firm’s larger cybersecurity strategy. It’s vital to ensure that vendors that have access to your data also have a robust risk posture. As firms add more vendors, they need to consider:

- How does the vendor approach cybersecurity?
- Does the vendor have risk remediation strategies?
- Does the vendor have an existing risk management process?

Firms need to have standards and systems in place to manage third-party security risks. New risks are always emerging, so it's important to regularly assess vendors to ensure they're evolving their controls over time.

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.

Ensuring processes, procedures, reporting and recordkeeping are a part of your larger cybersecurity framework. While it's true that IT leads cybersecurity initiatives, firms need to recognize that regulatory agencies are making cybersecurity a priority. Compliance and IT teams need to work together to prevent gaps in accountability.

Compliance team's role in cyber and vendor risk compliance

A plan for collaboration between compliance and IT teams needs to be implemented for both cybersecurity and vendor risk management. However, this doesn't just affect those who are managing processes and procedures. Reporting in plain terms to board members will be important so they can understand and make decisions based on current and future risks.

Compliance teams play a critical role in demonstrating cyber and vendor risk compliance to board members and regulators:

> **"Cybersecurity incidents can lead to significant financial, operational, legal, and reputational harm for advisers and funds. More importantly, they can lead to investor harm. The proposed rules and amendments are designed to enhance cybersecurity preparedness and could improve investor confidence in the resiliency of advisers and funds against cybersecurity threats and attacks."**
>
> - SEC Chair Gary Gensler statement on the proposed SEC cybersecurity rule

Review policies and procedures against gaps:

- Cybersecurity incident response and recovery
- Risk assessments
- User security and access
- Threat and vulnerability management
- Information protection
- Annual review and reporting

Ensure recordkeeping:

- Vendor risk assessments
- Cyber incidents
- Policies and procedures
- Board oversight
- Reports
- Reviews

Complete and file appropriate disclosures:

- Form ADV
- Fund registration statement
- Fund prospectus
- Fund annual reports

Report significant incidents:

- Form ADV-C

So what does this all mean?

With SEC regulations on the horizon, firms 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.

How Smarsh can help

Regulators have made it clear that there will be no debate when it comes to data security. Firms have the fiduciary duty to apply practices that are in the best interest of their clients, including taking steps to minimize cybersecurity risks that could lead to significant business disruptions and harm to investors.

Smarsh simplifies compliance by automating review workflows. Our software and services are purpose built to meet compliance obligations (FINRA, SEC, NIST, GDPR and more), so financial services firms have the tools they need for success.

Monitor devices, users, networks and vendors continuously through a single-pane-of-glass platform. This includes a standard incident response template to log cybersecurity incidents for investigation and remediation.

Whether firms need to demonstrate cyber and vendor compliance to regulatory agencies, or a comprehensive cybersecurity and vendor risk solution, Smarsh empowers firms' compliance teams to cost-effectively stay on top of regulatory requirements.

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.

Smarsh provides marketing materials for informational purposes only. Smarsh does not provide legal advice or opinions. You must consult your attorney regarding your compliance with applicable laws and regulations.

Guide - 10/22

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

© 2022 Smarsh, Inc. All rights reserved