Compliance Challenges for CISOs and Security Leaders in 2024

Learn more about upcoming cyber risk, vulnerability management, and third-party risk requirements.

Security leaders working in financial industries will face many new compliance regulations. Some will require companies to uplevel their threat intelligence programs; others contain updated definitions and more detail where there were none before. Other updates will have a profound effect on your cyber-risk strategy, especially as it pertains to your supply chain and third-party services.

Unsurprisingly, compliance regulations are starting to catch up to our customers' threat environment. Financial services are, by far, the most targeted industry by bad actors and subject to a crushing wave of compliance updates.

Some of the research we looked at tells a compelling story about security leaders' challenges. In one survey, 43% of cyber risk professionals said that their bank may not be equipped to protect customer data and privacy if there were a cyberattack.

However, less than half (47%) of those surveyed said their company planned to invest more in cybersecurity in 2023/24. The survey also indicated that banking executives were more concerned about cyber than credit risk. It is a rather sobering statistic considering the economic uncertainty we are currently experiencing.

We also just completed a study of five top financial institutions around the globe. We wanted to understand better the areas of cyber risk within the financial service environment, including third-party risk. Our study, Top Financial Institutions & Third-Party Risk, seeks to answer the question, "How much cyber risk are financial institutions exposing themselves to today?

It is an excellent read for any security leader who wants to learn more about security risks, weaknesses, and financial institutions' external digital risk landscape.

Given the regulatory environment that our financial customers will be entering this year and some of the results from our study, we wanted to offer some additional perspective on compliance updates that security leaders need to plan for in 2024. Examining

compliance is essential to assessing risk exposure and quantifying cyber risk, especially for financial services organizations.

Keep reading if you are a CISO, SOC leader, or manage your company vulnerability program. Some updates are effective today, and you already know about them; others may not be effective until early 2025. Either way, you need to start thinking about how the upcoming changes apply to you, including:

- Guidance and definitions for risk assessments and vulnerability scans
- Frequency and scope of vulnerability scanning
- 3rd party assessment and breach disclosure

What Security Leaders need to know about Compliance & Third-Party Cyber Risk

When we studied five global banks to determine their attack surface and exposure, we found that, on average, 75% of vulnerabilities were associated with third-party platforms.

When you consider that in 2022 CVE.ICU reported a 25% YOY increase in CVEs with an average of 69 per day and a CVSS score above seven; the need for compliance updates becomes well understood. Another study that caught our attention was from SANS; it indicated that less than half (43%)of the vulnerability management professionals surveyed manage supply chain vulnerabilities.

CISOs Keep Your Eyes on DORA in 2024

On the surface, the upcoming EU Digital Operational Resiliency Requirements (DORA) regulations may seem benign. Like many newly established compliance updates and regulatory measures, they do not tell you how to comply, only what is expected. So, it's up to you to decide how you want to comply with the requirements of a "risk-aligned approach." Security leaders have much leeway to meet the needs of third-party risk. However, that is only half the story.

The risk assessment section of the new legislation does not show DORA's teeth. DORA's power is in the digital operational resiliency requirements. This section spells out the resiliency, impact tolerance, and regular end-to-end recovery testing in your organization in alignment with your supply chain partners and third parties involved with the delivery of financial services to EU organizations and consumers.

DORA addresses pandemics, technology outages, and natural disasters to strengthen an organization's response to business disruption. In the case of cyber incidents, you cannot recover if you don't know it happened. It is especially true when it concerns third-party infrastructure, where you may or may not have visibility. So, DORA will place some additional requirements on CISOs to not only be able to respond to supply chain cybersecurity events but also holistically recover from any impact.

NYDFS Expands Notification Requirements

The New York Department of Financial Services recently approved an amendment to 23 NYCRR Part 500, a regulation establishing cybersecurity requirements for financial services companies. Starting November 1, 2023, covered entities must notify NYDFS of a cyber incident with a third-party provider, even if the provider has already notified NYDFS. This requirement applies to all covered entities even if the Third-Party Service Provider also notifies DFS. It applies to all DFS-authorized financial service branches, agencies, and representative offices of out-of-country foreign banks.

Compliance Updates Require Increased Risk and Vulnerability Assessments in 2024

We could not help but notice many compliance updates and requirements that call for increased risk assessment, vulnerability scanning, and asset inventory. All compliance updates will require increased frequency, with many stating that you will now need to perform vulnerability scans in response to any changes made to your environment. Compliance requirements are rapidly moving from annual or triannual assessment and point-in-time efforts like penetration testing to a more continuous threat exposure management approach.

Let's look at new updates requiring frequent or continuous monitoring for unsecured exposure and vulnerabilities.

As mentioned, the New York Department of Financial Services (NYDFS) amended 23 NYCRR Part 500. The approved amendment reduces the vulnerability assessment and testing requirement from three years to every six months, or the organization will need to implement a continuous monitoring program.

In April 2023, Binding Operational Directive 23-01 became effective. Among other mandates, it requires our Federal government to perform automated asset discovery every seven days.

In June 2023, the Safeguards Rule, an update to the Gramm-Leach-Bliley Act (GLBA), became effective. It updated the requirements for protecting customer financial information and now covers a wide range of industries that handle sensitive consumer information. Covered entities must employ continuous threat and exposure monitoring of their systems. Without that capability, you must conduct system-wide scans every six months.

Don’t Overlook New Requirements for PCI 4.0 Compliance

A much-needed definition of a vulnerability scan is included with PCI 4.0, where there was little guidance. Upleveled requirements will demand more robust vulnerability scanning, including:

Requirement 11.3.1.2 (March 31, 2025)

Authenticated scans—Vulnerability scanners must be able to use credentials to gain access to exposed web applications and test ports and services for weaknesses.

Secure Credential Storage—In the past, if you stored sensitive authentication data before authorization of a vulnerability scan, it was suggested that you encrypt and protect the credentials. Now, the scanner is required to provide authenticated vulnerability scans.

Requirement 4.2.1 (March 31, 2025) – Certificate tracking This update requires your security team to track and inventory all 509 certificates for transmitting sensitive data across public networks.