Skadden

Cybersecurity and Data Privacy Update

October 29, 2026

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum is considered advertising under applicable state laws.

One Manhattan West
New York, NY 10001
212.735.3000

The New Cyber Incident Response Playbook: How Evolving Requirements in the EU and US Have Changed the First 72 Hours

Executive Summary

- **What's new:** Expanding regulatory regimes in the U.S. and EU, including NIS 2, DORA, CRA, amended Regulation S-P and SEC rules, are compelling organizations to reassess their approach to handling the first 72 hours of a cyber incident.
- **Why it matters:** A single cyber incident can now start multiple notification clocks at the same time. This affects critical infrastructure, financial entities, digital product manufacturers, covered financial institutions and public companies. Management may also face personal liability.
- **What to do next:** Companies should consider refreshing incident response plans to build in the additional notification assessments, and stress testing them during privileged tabletop exercises. They can also establish rapid escalation protocols, and keep records of when incidents were discovered, escalated and assessed.

Introduction

Expanding regulatory regimes in the U.S. and EU are compelling organizations to reassess their approach to handling the first 72 hours of a cyber incident. In the EU and U.K., companies must assess whether notification triggers are met under new and overlapping cybersecurity regulations, including the Network and Information Security Directive 2 (NIS 2), Digital Operational Resilience Act (DORA) and Cyber Resilience Act (CRA).

In the U.S., Regulation S-P requires covered financial institutions to maintain procedures designed to ensure service providers inform them of data breaches within 72 hours, with covered institutions themselves having to notify affected individuals with compromised sensitive data as soon as practicable and at latest within 30 days of learning of the breach. Securities and Exchange Commission rules also require domestic public companies to assess materiality without unreasonable delay and disclose material incidents within four business days of that determination.

With both the frequency of cybersecurity incidents and the intensity of regulatory authority and scrutiny sharply increasing, management teams should consider implementing procedures to quickly and effectively assess whether a cyber incident has triggered new notification requirements.

© Skadden, Arps, Slate, Meagher & Flom LLP. All rights reserved.

The New Cyber Incident Response Playbook: How Evolving Requirements in the EU and US Have Changed the First 72 Hours

EU Regime	Scope	Breach Notification Trigger
NIS 2	Imposes cybersecurity obligations across critical infrastructure sectors	Where a cyber incident has a "significant impact" on the provision of its services, a regulated entity must submit an "early warning" to regulators within 24 hours and an "incident notification" within 72 hours of becoming aware of the incident. For more information, see our NIS 2 article "Key Implications of the EU's NIS 2 Directive."
DORA	Requires financial entities to implement heightened security and resilience measures	Regulated entities must notify regulators within 24 hours of any "major information and communication technology (ICT)-related incident," followed by an "intermediate report" within 72 hours of the initial notification. For more information, see our DORA article "Key Considerations for Alternative Investment Funds."
CRA	Obliges producers of certain digital products to comply with a range of cybersecurity requirements	Manufacturers of covered products must notify regulators within 24 hours of any actively exploited vulnerabilities or incidents that compromise or could compromise data on that product. For more information, see our CRA article "Reporting FAQs and Checklist as the EU's Cyber Resilience Act Comes Into Force."

What's New in the EU

The new cybersecurity laws go beyond personal data under the familiar General Data Protection Regulation (GDPR). A single cyber incident can now start GDPR, NIS 2, DORA and CRA clocks at the same time, each with its own scope and trigger for breach notifications. The chart above provides an overview of these new regimes.

Reporting obligations under the CRA are the latest addition to the notification obligations companies face in the first 72 hours. Companies should therefore consider assessing whether they and/or their products fall within scope before a reportable incident occurs, given that the first notification is due within 24 hours.

In addition to breach notification obligations, both DORA and NIS 2 expose members of management bodies to personal liability. Board members cannot discharge this responsibility simply by delegating oversight of cybersecurity and ICT risk management to the chief information security officer (CISO). The precise form of liability is determined by national law: Under DORA, for example, fines on individuals can reach €5 million in some jurisdictions. Board members therefore may wish to undertake regular, documented cybersecurity training to keep their knowledge up to date.

What's New in the US

Accelerated Reporting Obligations and SEC Priorities Raise the Stakes for Public Companies and Covered Financial Institutions

Compliance with amended Regulation S-P became mandatory for larger covered institutions on December 3, 2025. The amendments address covered institutions' incident response programs, as well as oversight of service providers, including procedures designed to ensure service providers notify institutions of certain breaches within 72 hours. Covered institutions must maintain written incident response programs designed to assess the nature and scope of an incident, achieve containment and provide required notifications. Subject to limited exceptions, institutions must notify individuals whose sensitive customer information was affected as soon as practicable, and at latest within 30 days of learning of a breach.

Moreover, covered institutions must maintain written oversight policies and procedures reasonably designed to ensure service providers (1) protect against unauthorized access to or use of customer information and (2) notify the covered institution as soon as possible, but no later than 72 hours after becoming aware of a breach.

Separately, public companies continue to contend with the SEC's cybersecurity disclosure rules, which require domestic public companies to quickly assess and determine whether cybersecurity incidents are material without unreasonable delay following discovery. Under Item 1.05 of Form 8-K, materiality is assessed under the traditional securities law standard, considering whether

a reasonable investor would view the incident as important to an investment decision. Once an incident is determined to be material, companies must generally disclose the material aspects of its nature, scope, timing and material or reasonably likely material impact within four business days of the determination.

The SEC has identified compliance with Regulation S-P and safeguarding of customer records as examination priorities for 2026 — with a particular focus on companies' operational resiliency, ransomware response capabilities, and training to mitigate new risks from artificial intelligence (AI). In November 2025, the SEC settled charges against M Holdings Securities, Inc. under Regulation S-P's pre-amendment safeguards rule, citing deficiencies in multifactor authentication, security training and incident response policies. More recently, on August 19, 2026, the SEC secured a final judgment against a California-based investment adviser based in part on violations of Regulation S-P related to the investment adviser's unauthorized retention of nonpublic customer information while attempting to leave his current employer to start his own investment advisory firm. While neither of these enforcement actions was initially brought under the amended Regulation S-P, they provide instructive examples of the types of violations that have given rise to SEC scrutiny in the past — and the amended rules regarding written incident response programs, customer notifications and service provider oversight will only expand the scope of conduct that could give rise to enforcement actions.

Covered institutions should consider reviewing their incident response programs to ensure they are designed to comply with the amended reporting requirements. Companies will want to be well-poised to quickly assess potential notification obligations in the immediate aftermath of an incident and take steps to mitigate the potential for regulatory enforcement, litigation or reputational impact.

Heightened Expectations for Rapid Escalation and Board and Senior Management Oversight

Regulators increasingly expect corporate boards to quickly assess potentially significant incidents, and management to implement procedures to promptly escalate information to and seek engagement from boards. The SEC rules (Regulation S-K) require annual disclosures describing cybersecurity risk management processes and board oversight and management's role in assessing and managing material cybersecurity risks, including how boards are informed of such risks. The provisions in the amended Regulation S-P requiring service providers to escalate certain incidents within a short 72-hour timeline have accelerated the speed at which companies are expected to assess and report cyber incidents generally.

Separately, the New York State Department of Financial Services (NY DFS) also requires covered entities to report certain incidents to NY DFS within 72 hours after determining they occurred. NY DFS has emphasized the importance of active oversight of cybersecurity risk by covered entities' senior governing bodies, recommending that directors and officers have sufficient understanding of cybersecurity-related matters and the ability to provide a "credible challenge" to management's cybersecurity decisions.[1] NY DFS specifically emphasizes the necessity of oversight in view of the expanded attack surface created by covered entities' reliance on advanced technologies — such as cloud computing and AI — that are often managed by third-party service providers.

To keep apace with heightened regulatory expectations, boards should consider requesting regular briefings on AI and third party dependencies and the associated risks. Policies and procedures can also establish rapid escalation protocols for operational disruption, significant data exposure, ransom demands or other potentially material consequences that may warrant board involvement.

What Companies Should Consider Now

- Refresh incident response plans to ensure additional applicable notification assessments are incorporated into the early stages of the incident response process — organizations may wish to stress test these processes during privileged tabletop exercises.
- Remain abreast of relevant regulations as they evolve — for example, the EU's Digital Omnibus introduces wide-ranging measures aimed at reducing the burden of the EU's digital legislative framework (see more information in our November 21, 2025, client alert "Commission Proposes Significant Changes to EU Digital Rules – First Impressions"). Increasing enforcement of cybersecurity regulations will also clarify the aspects of these and other wide-ranging laws to which regulators are paying closest attention.
- Maintain appropriate documentation of when incidents were discovered, escalated and assessed for materiality or notification, including the basis for decisions, to support regulatory examinations and litigation defense.
- Prepare a comprehensive incident response program designed to facilitate quick assessment of the potential operational, financial, reputational and legal consequences — which will help support the materiality assessment process and other rapid reporting obligations. The assessment need not await completion of a forensic investigation if sufficient information is available to determine materiality.

[1] New York State Department of Financial Services. (October 1, 2025). "Guidance on Managing Risks Related to Third-Party Service Providers" [Industry Letter].

The New Cyber Incident Response Playbook: How Evolving Requirements in the EU and US Have Changed the First 72 Hours

Contacts

Nicola Kerr-Shaw
Partner / London
44.20.7519.7101
nicola.kerr-shaw@skadden.com

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Kyle G. Kysela
Associate / Chicago
312.407.0546
kyle.kysela@skadden.com

Alex Smallwood
Associate / London
44.20.7519.7202
alex.smallwood@skadden.com

Dimitri Vallejo
Associate / New York
212.735.3384
dimitri.vallejo@skadden.com

Brittany Wong
Trainee Solicitor / London
44.20.7519.7448
brittany.wong@skadden.com