POLSINELLI

# Publications

January 7, 2025 • Updates

## Cybersecurity Compliance in 2025 – Know Your "Technology" Assets

"Has World War III Already Begun?" That was the headline for an article by the chief foreign-affairs correspondent for the Wall Street Journal last month, which reported how Russia is "getting even more effective at using new tools, like cyberattacks and ransomware, to disrupt our societies."

China is too. A year ago, the FBI Director warned that China was ramping up an extensive hacking operation designed to take down the United States' power grid, oil pipelines and water systems. Then in April 2024, the director reaffirmed this while speaking at the *Modern Conflicts and Emerging Threats* summit in Nashville:

"The PRC [People's Republic of China] has made it clear that it considers every sector that makes our society run as fair game in its bid to dominate on the world stage, and that its plan is to land low blows against civilian infrastructure to try to induce panic and break America's will to resist."

Even with alarm bells sounding, it was shocking to learn in October 2024 that China had hacked into multiple telecommunications companies and stolen vast amounts of sensitive data and confidential information. Worse yet, it is still unclear what the full extent of China's theft has been and how long intruders have been inside the companies' networks.

Given these and other complex threatscape scenarios, it is not surprising that 2025 is expected to be an important year for cybersecurity laws and regulations. On December 27, addressing the fallout from China's hacking campaign on the telecom industry, a White House spokesperson suggested that *voluntary* cyber security practices have been inadequate.

### *What Was Voluntary, May Become Mandatory*

Speaking of voluntary, in 2020 while the world was in the throes of the pandemic and threat actors exploited new security risks relating to remote work, the Department of Health and Human Services Office for Civil Rights (OCR) provided important guidance relating to mandatory risk analyses required under the Health Insurance Portability and Accountability Act (HIPAA).

### Related People

- Bruce A. Radke
- ILIANA L. PETERS
- Michael J. Waters
- Romaine C. Marshall

### Related Capabilities

- Privacy & Cybersecurity
- International Privacy
- Data Breach & Incident Response

Noting that OCR investigations frequently find that organizations lack sufficient understanding of where their sensitive and personal information (i.e., regulated data) is located, OCR stated that creating and maintaining an up-to-date, IT asset inventory "could be a useful tool" in assisting with risk analysis compliance.

OCR then described in some detail what inventorying entails, including IT Asset Management (ITAM) solutions. OCR referred also to components of the NIST Cybersecurity Framework, a reliable set of guidelines and practices that organizations can customize to their needs and that some states have included in their cybersecurity laws.[1]

Instructively, OCR went on to explain that understanding one's environment—particularly how personal and sensitive information is created and enters an organization, flows through an organization and leaves an organization—is crucial to understanding the risks that information is exposed to throughout one's organization.

When creating an IT asset inventory, OCR encouraged organizations to include, in summary, the following:

- Hardware assets, including electronic devices and media, which make up an organization's networks and systems.
- Software assets that run on an organization's electronic devices such as anti-malware tools, operating systems, databases, email, administrative and financial records systems.
- Data assets that an organization creates, receives, maintains or transmits on its network, electronic devices and media.

Recently, other agencies have recommended or required the same. For instance, several weeks ago the Federal Trade Commission finalized an order with Marriott International, Inc. In addition to the standard requirements, Marriott must also "establish, implement, and maintain scanning or equivalent tools to regularly inventory and classify Marriott IT assets containing Personal Information that includes hardware, software, and the location of any such Marriott IT assets."

Similarly, the Critical Infrastructure Security Agency recommends as a "highest-priority baseline" that covered entities of all sizes maintain a regularly updated inventory of all organizational assets including Operational Technology (not just IT) on a recurring basis, but nothing less than a monthly basis.

A few weeks ago, OCR issued a Notice of Proposed Rulemaking (NPRM) to modify the HIPAA Security Rule as part of its support for the Biden-Harris National Cybersecurity Strategy, which is an extension of what the previous Trump administration unveiled. The last time the Security Rule was modified was in 2013.

Notably, according to an OCR Fact Sheet also released on December 27, the NPRM revisions to the Security Rule could require:

- Developing and revising a technology asset inventory and network map at least every 12 months.
- Mandatory analysis of a technology asset inventory and network map, as part of the Security Rule's risk analysis requirement.
- Analysis of the relative criticality of relevant electronic information systems and technology assets to determine their priority for restoration when an incident happens, as part of the Security Rule's risk analysis requirement.

Public comments on the NPRM are due 60 days after its publication in the Federal

Register on January 6, 2025.

## *Call to Action*

We have noted on numerous occasions that developing and implementing an incident response plan, conducting periodic risk assessments and having an updated written information security program are important components to effective cybersecurity compliance.[3] This is sometimes easier said than done, especially as organizations' environments evolve and expand.

Organizations should consider whether their policies, procedures and plans enable them to fulfill cybersecurity requirements by regularly inventorying their technology assets—to first *know* their assets—and especially in relation to the data and information they manage. Sources cited herein provide guidance. Reach out to the authors if you need related legal advice.

[1] *See, e.g.*, Utah's Cybersecurity Affirmative Defense Act providing a 'safe harbor' for organizations that get hacked and then sued for negligence, if they have implemented a written information security program that maps to the NIST CSF or other frameworks.

[2] *See* Polsinelli's discussion of the strategy here and an update here.

[3] *See, e.g.,* Polsinelli's discussions of cybersecurity recommendations for 2023 (February 2023), changes to cyber incident reporting for the Critical Infrastructure Act (March 2023) and evolving incident response obligations (April 2024).