Cybersecurity: Regulators show their teeth

New formal cybersecurity standards covering US financial institutions could have ramifications that reach far beyond New York.

US regulators usually issue cybersecurity guidance instead of regulator standards and requirements. That changed on March 1, 2017, when the Superintendent of New York's Department of Financial Services (NYDFS) exceeded federal efforts and put into effect Cybersecurity Requirements for Financial Services Companies (Cybersecurity Regulation).

Following a spate of cyber-attacks and breaches of customer confidentiality, the NYDFS declared that for certain financial institutions operating in New York "regulatory minimum standards are warranted". Although this edict directly applies only to banks, insurance companies and other financial services institutions specifically regulated by the NYDFS, (i.e., with operations subject to the jurisdiction of the NYDFS), financial institutions are finding that the requirements may apply indirectly to foreign headquarters and branches located throughout the world.

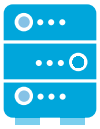
Purpose and requirements

The Cybersecurity Regulation is an ambitious regulatory initiative not limited to protecting consumer privacy. Rather, by focusing on all nonpublic information (including business confidential information unrelated to individuals) as well as on network stability, the NYDFS requires that its regulated entities, "ensure the safety and soundness of the institution," while also protecting their customers. The Cybersecurity Regulation was promulgated to address the growing concern of financial industry regulators with the vulnerability of personal, financial and business data processed by NYDFS-supervised organizations and to protect the associated level of security of their information technology systems against systemic harm. The NYDFS's methodology for entities to achieve the agency's desired result involves a mix of risk management principles and compliance demands. At its core, the Cybersecurity Regulation requires an extensive list of regulated entities to implement and maintain a thorough 14-point cybersecurity policy with requirements that range from asset management to incident response. Covered organizations (and individuals) are required not only to consider "relevant risks" to their business, but also to "keep pace with technological advances."

> **Cybersecurity Regulation may apply indirectly to foreign branches of financial institutions**

The minimum standards imposed on organizations and individuals under the Cybersecurity Regulation address several areas, including:

- Requiring certain physical, administrative and technical controls to ensure that an organization's cybersecurity program addresses cybersecurity risks, and protects nonpublic data and the information systems, including written cybersecurity policies and procedures, encryption, multi-factor authentication, penetration testing and risk assessment
- Implementing a corporate governance framework that involves participation and oversight at all levels —from vendors to the board of directors —and requires reporting to executive management on evolving cybersecurity risks to facilitate necessary revisions to the cybersecurity program
- Submitting an annual certification, prepared by executive management, to the Superintendent of the NYDFS confirming compliance with the Cybersecurity Regulation, and documenting necessary material improvements to the cybersecurity program



14-point

Cybersecurity Regulation calls for a 14-point cybersecurity policy for all regulated entities

Developing and implementing a written incident response and remediation plan addressing internal incident response processes, goals of the response plan, delineation of clear roles and responsibilities for incident response decision-making authority, external and internal communications, requirements for remediating cybersecurity weaknesses, cybersecurity event and incident response documentation and reporting, and evaluation and revision of the plan. Some organizations may qualify for relief from certain or all compliance obligations under the Cybersecurity Regulation if they fall under one or more of nine exemptions. These exemptions

may be available based on the size of an organization, reliance on the cybersecurity program of another related entity, access or control over nonpublic information or information systems, or designation as a special insurance or reinsurance entity. Absent an exemption, organizations that fail to comply with the Cybersecurity Regulation may be subject to penalties and enforcement actions by the Superintendent of the NYDFS under existing law.

Global reach

Importantly, the Cybersecurity Regulation has an extraterritorial reach that extends well beyond the regulated entity itself. Typically, many large enterprises gain business efficiencies and closer coordination between their subsidiaries and affiliates by deploying a unified information technology platform with centrally managed security. Thus, if a segment of the enterprise, however small, falls under the jurisdiction of the NYDFS, the enterprise's broader program may effectively fall under its watchful eye and will have to meet the Cybersecurity Regulation's requirements to the full extent it is relied upon by the enterprise's NYDFS-regulated entity. In these instances, all the relevant documentation and information about the larger program must be made available to the NYDFS upon its request. Similarly, when regulated entities use vendors, NYDFS requirements exist to ensure the appropriate level of security for the information and systems that are accessible to, or held by, third-party service providers.

For foreign organizations with branches, employees, subsidiaries or affiliates operating in New York State, the reach of the Cybersecurity Regulation warrants full attention and consideration. If a foreign organization determines that the Cybersecurity Regulation applies to its affiliates, third-party service providers or employees operating in New York, then the organization could be beholden to the NYDFS for cybersecurity program inquiries. This could mean, for example, that a foreign-based organization's overall cybersecurity program documents and practices may be open for review and inspection by the Superintendent of the NYDFS based on its New York operations thousands of miles away from its core and broader operations and activities, including across multiple jurisdictions. It could also mean that foreign third-party vendors who provide cybersecurity program services to the organization or its affiliates may be subject to certain obligations under the Cybersecurity Regulation.

> **Cybersecurity Regulation has an extraterritorial reach that extends well beyond the regulated entity itself**

This potential reach of the Cybersecurity Regulation raises legitimate jurisdictional concerns about a local regulator's ability to obtain insight into the network security of a global enterprise, regardless of where the company is headquartered. In addition, foreign companies could begin to see compliance costs rise due to conflicting cybersecurity standards set forth under other laws, such as the General Data Protection Regulation, or if other states in the US, or other countries, begin to promulgate similar regulations that are not harmonized with New York's Cybersecurity Regulation. Thus, companies should be aware that aspects of their enterprise-wide cybersecurity programs and controls could come under the ambit of the NYDFS and prepare accordingly. For enterprises with significant worldwide operations, failing to appreciate the potential reach of the NYDFS under the Cybersecurity Regulation could present significant issues.

72-hour incident reporting

The Cybersecurity Regulation also requires covered entities to notify the superintendent within 72 hours of its determination that an act or attempt, whether or not successful, was made to gain unauthorized access to, disrupt, or misuse, an information system or the information stored on it, to the extent that (a) notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (b) the event has a reasonable likelihood of materially harming any material part of the entity's normal operations. To determine whether an unsuccessful act or attempt is reportable, organizations will want to consider whether defending against it was routine in nature or required taking measures "well beyond" those ordinarily used.

C-suite-level involvement

The significance of the global reach and tight 72-hour incident reporting timetable of the Cybersecurity Regulation is amplified by the requirements placed on officers and directors of a covered foreign organization to oversee and manage the cybersecurity program applicable to its New York operations, and to document their review, understanding and approval of the program. Should the NYDFS request a review and access to an organization's cybersecurity program, the role and involvement of the organization's officers and directors in implementing the program will come under scrutiny. Therefore, in addition to appreciating the extraterritorial reach of the Cybersecurity Regulation outside of New York, senior officers (and boards of directors) should focus on the following obligations: ESMA anticipates that legal questions will arise as the technology develops and its applications become more visible. It believes that it is too early to gain a complete understanding of the changes that the technology may introduce and that any regulatory action would be premature.

- Review and approve the organization's written cybersecurity policy and ensure that it addresses the specifically enumerated topics under the Cybersecurity Regulation. The cybersecurity program should consider not just personally identifiable information, but all

Enforcement actions againts US-based entities may implicate foreign interests on a potentially much larger scale than many firms may reasonably anticipate

nonpublic business-related data as well as the resilience of key systems

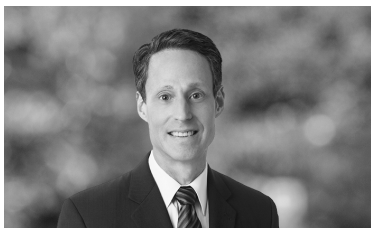
- Confirm that the annual report from the chief information security officer (CISO) is generated and provided to the Board. The Cybersecurity Regulation specifically requires the CISO to provide a written report to the directors on the cybersecurity program and any material risks
- Ensure that the organization's risk assessments, third-party service provider policies, and incident response and remediation plans are tracked and documented. This documentation is necessary for officers and directors to annually certify that they have reviewed the documentation and that the organization's cybersecurity program is compliant with the Cybersecurity Regulation. Should the superintendent request review of the cybersecurity program, then the documentation provides proof of compliance
- Become familiar with the organization's existing documentation procedures and adjust as necessary. Executive management should seek guidance on how to limit documentation only to what is necessary to show compliance, taking into account any applicable legal privileges

Vigorous compliance

The Cybersecurity Regulation is intended to protect individual and business-confidential information related to financial institutions, and the integrity and availability of such data, as well as an organization's networks and applications. In promulgating the Cybersecurity Regulation, the NYDFS is attempting to protect a critical infrastructure important to New York—the banking and finance industry. As a result, the NYDFS is expected to vigorously pursue and monitor compliance with the Cybersecurity Regulation, which could result in enforcement actions against US-based entities that may implicate foreign interests on a potentially much larger scale than many firms may reasonably anticipate. Based on recent history, the New York operations of non-US banks have been a frequent target of the NYDFS (with respect to other issues, to include anti-money laundering and sanctions compliance programs and enforcement); it is reasonable to assume these institutions will continue to be within the NYDFS's sights. Given the extraterritorial reach of the Cybersecurity Regulation and the NYDFS's willingness to exercise its reach in other contexts, organizations near and far should take heed, and be prepared to act quickly.

Kevin Petrasic
Partner, Washington, DC

T +1 202 626 3671
E kevin.petrasic@whitecase.com



Steve Chabinsky
Partner, New York

T +1 212 819 8718
E steven.chabinsky@whitecase.com

F. Paul Pittman
Associate, Washington, DC

T +1 202 626 2395
E paul.pittman@whitecase.com

whitecase.com