AN **ALERT** FROM THE BDO FINANCIAL SERVICES PRACTICE

BDO KNOWS:

CYBERSECURITY

FIRST PROPOSED STATE-ISSUED CYBERSECURITY RULES TO GOVERN NEW YORK DEPARTMENT OF FINANCIAL SERVICES-REGULATED ENTITIES

SUMMARY

On Sept. 13, New York Governor Andrew Cuomo issued proposed cybersecurity regulation for financial services entities regulated by the New York Department of Financial Services (NYDFS)—the first to impose cybersecurity requirements at the state or federal level, but likely not the last.

NYDFS regulates state-chartered institutions and foreign banks licensed to operate in New York, as well as all insurance companies that do business in the state.

The proposed rules aim to ensure NYDFS-regulated entities safeguard consumer and other sensitive information by implementing policies and procedures for cyber risk and incident detection, response and recovery. Central to reinforcing these core functions are the proposed regulation's requirements to establish a written cyber policy, designate a Chief Information Security Officer (CISO) to oversee and enforce adequate programs, address third-party risk and perform regular penetration tests and assessments.

DETAILS

Financial services—the third most-attacked industry in 2015—is no stranger to the cyber threat. It's widely known that cyber incidents can cause significant financial and reputational harm to financial services institutions and insurance companies that house troves of sensitive consumer, transactional and other classified data. This regulation—if implemented—will become the nation's first mandate to require adherence to certain minimum cyber standards and hold organizations accountable for their role in the battle against cybercrime.

Specifically, the proposed requirements—now open for a 45-day comment period and subject to change before final issuance—mandate that NYDFS-regulated entities:

- **Establish a cybersecurity program** designed to ensure the confidentiality, integrity and availability of information systems that perform five core cybersecurity functions: identify cyber risks, implement policies and procedures to protect unauthorized use or access, detect cybersecurity events, respond to cybersecurity incidents, and restore normal operations and services following an attack.
- **Adopt a written cyber policy** that sets forth policies and procedures to protect information systems and nonpublic information that address, minimally: information security; data governance and classification; access controls and identity management; business continuity, and discovery planning and resources; capacity and performance planning; systems operations and availability concerns; systems and network security, monitoring and quality assurance; physical security and environmental controls; customer data privacy; vendor and third-

BDO'S FINANCIAL SERVICES PRACTICE

BDO's Financial Services Practice draws on deep industry experience to help clients navigate a changing and highly competitive industry. Our professionals deliver audit, tax, and consulting services to a wide range of financial institutions, asset managers, broker dealers, and insurance companies. We provide proactive guidance and value-added services to our clients, including comprehensive compliance and litigation support services.

ABOUT BDO USA

BDO is the brand name for BDO USA, LLP, a U.S. professional services firm providing assurance, tax, advisory and consulting services to a wide range of publicly traded and privately held companies. For more than 100 years, BDO has provided quality service through the active involvement of experienced and committed professionals. The firm serves clients through more than 60 offices and over 500 independent alliance firm locations nationwide. As an independent Member Firm of BDO International Limited, BDO serves multi-national clients through a global network of 1,408 offices in 154 countries.

BDO USA, LLP, a Delaware limited liability partnership, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms. BDO is the brand name for the BDO network and for each of the BDO Member Firms. For more information please visit: www.bdo.com.

Read more ▶

party service provider management; risk assessment; and incident response.

- **Designate a qualified CISO** responsible for overseeing and implementing the institution's cybersecurity program and enforcing its cybersecurity policy. The CISO will be required to report to the board at least biannually.
- **Implement a formal third-party cyber risk management program** by implementing policies and procedures that identify and assess the risk of third parties with access to information systems or nonpublic information; ensure compliance with minimum cybersecurity practice requirements; confirm strong due diligence processes are used to evaluate the adequacy of third parties' cybersecurity practices; and periodically assess (at least annually) third parties and the continued adequacy of their cyber practices.

Additional requirements outline rules for penetration testing and vulnerability assessments, transactions and log access privileges, employment and training of cybersecurity personnel, multi-factor authentication for individuals accessing internal systems, destruction of unnecessary nonpublic information and encryption of all nonpublic information held or transmitted.

The proposal—while requiring financial institutions and insurance companies to meet certain minimum standards—aims to provide enough flexibility to avoid constraining industry innovation and allow firms to design their own programs based on their unique needs.

INSIGHTS

Guidance from regulators has existed for some time, but the mandatory compliance of this proposed regulation, and the intended fast-track to issuance, make it a game changer. Banks, insurers and other financial institutions—particularly those based in New York—are subject to increasing risk. If organizations do not prioritize cybersecurity, this risk could escalate to national security and economic issues.

How the regulation evolves throughout the 45-day comment period remains to be seen, but BDO recommends that organizations operating under the NYDFS jurisdiction consider its potential impacts, including:

- **Board involvement:** Given that the regulation requires CISOs to report to their boards biannually, and senior officers are mandated to sign off on and submit a compliance certificate, the rules force boards to get involved. And when cybersecurity is embraced as a corporate priority at the highest level, the organization is better positioned in terms of readiness and resilience.
- **Management of third-party vendors:** A broad vendor base is common among financial institutions, and identifying and mitigating potential vulnerabilities throughout their extended networks is vital. The proposed regulation's rigorous requirements mean organizations will need to demonstrate diligence and proactive outreach to their vendors to ensure they, too, are prioritizing cybersecurity.
- **Compliance burdens:** Some larger banks and insurers may already have cybersecurity measures in place that meet the minimum requirements set forth by this new regulation. But smaller organizations may face larger burdens as they look to bring their programs and policies up to speed. It's important to note that one of the requirements with the seemingly greatest financial burden—designating a CISO—can be fulfilled by hiring an external, or "virtual," CISO.
- **Disclosure:** The 72-hour time frame to report a breach to the NYDFS would be the most aggressive reporting window of any state, significantly increasing the pressure on covered entities to be prepared and nimble. It's in all cyber players' best interest for notification standardization to ensure clarity around steps organizations need to take in the event of a breach, as crisis without planning often leads to chaos and mismanagement.
- **Regulators are targeting the financial services industry:** Between the SEC's OCIE Cybersecurity Examination Initiative, the FFIEC's cyber-extortion guidance and enforcement action from the CFPB, the financial services industry has been in the crosshairs of regulators' cyber efforts, though the level of scrutiny for small to mid-sized organizations compared to larger banks has been relatively inconsistent. The NYDFS has called for more coordination and collaboration between state and federal agencies in regulating cybersecurity at financial institutions—widely viewed as critical to the United States' national infrastructure and a top security priority. We may see industry regulators at the state and federal levels converge toward a consistent framework.

While the proposed regulation is limited to New York, we expect other state regulators and federal agencies will introduce similar requirements for financial institutions and other highly regulated industries. We believe the rules codify existing best practices that all financial institutions should already be adhering to.

BDO works with insurers and financial institutions to develop a comprehensive, holistic approach to cybersecurity and compliance, taking a 360-degree view of information risk and opportunity.

You can also read up on BDO's perspective on the NYDFS proposed regulation on Fortune.com, here.

For more information about how your organization can get ahead of the NYDFS-proposed cybersecurity regulation, please contact:

SHAHRYAR SHAGHAGHI
BDO Consulting Technology Advisory Services National Practice Leader and Head of International BDO Cybersecurity
sshaghaghi@bdo.com

IMRAN MAKDA
Co-leader of BDO's Insurance Industry Group
imakda@bdo.com

KEITH MCGOWAN
Leader of BDO's Asset Management Practice
kmcgowan@bdo.com

JIM CARTER
Leader of BDO's Financial Institutions & Specialty Finance Practice
jcarter@bdo.com