REGULATORY UPDATES

Three Steps to Address Regulatory Changes in 2023

By Ryan Spelman, Managing Director, Cyber Risk

Understanding Key Regulatory Changes

2023 brings changes in major regulatory requirements including New York State DFS (NY DFS), California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), and the Securities and Exchange Commission (SEC). While some of these changes may make modifications over the course of the year, no matter how you look at it, this year is going to be monumental for cybersecurity regulations and something every CISO and security leader needs to be thinking about. But more so, the leadership of organizations must spend time understanding what's in store and the business impact once these regulations come into effect.

Why does following regulations matter? Failing to meet regulatory requirements is costly. The average cost of fines for NYS DFS is about $10 million. In October 2022, they fined $4.5 million for failure to conduct periodic risk assessments, together with failure to implement multi-factor authentication and secure access controls, resulting in a breach that exposed New York consumer data. For CCPA/CPRA, the first public fine was $1.2 million due to a failure to comply with injunctive terms. The SEC has fined many organizations, one for almost $500,000 for disclosure controls and procedure violations related to a cybersecurity vulnerability that exposed sensitive customer information.



New York State Department of Financial Services CRR 500

NYS DFS was established in 2017, and the first state-level cybersecurity regulation for financial institutions. It covers all financial institutions regulated by NYS DFS, including mortgage companies, insurance companies, and state-chartered banks.

It is very prescriptive, requiring: naming of a "CISO" or equivalent, cybersecurity policy, penetration testing and vulnerability assessment, risk assessment, and annual Board certification.

New Regulations for NYS DFS Include:

- Tiers of enhanced requirements based on revenue and size of company. If you are a "Class A" company, you must have certain things in place such as audits, password control, monitoring, and an EDR solution. This is the first time an organization has been mandated to have an EDR solution in place.
- CISO independence. CISOs must have an adequate level of independence as it pertains to their authority, oversight, and decision-making.
- Greater Board responsibility. Previous iterations did not include Boards, but now the Board has to approve cyber policies, and have a certain level of cyber knowledge or resources to help show they understand the topics at hand.
- Expanded focus on Business Continuity and Disaster Recovery. This requires significant details regarding designations of certain personnel,

communications and more.

- Tailored Risk Assessments. They are enhancing risk assessment requirements with actual teeth behind what defines a risk assessment.

California Consumer Privacy Act/ California Privacy Rights Act

CCPA was created to avoid a constitutional change in policy and created GDPR-like state privacy requirements in 2018. CPRA was a constitutional change that provides greater clarity and creates an enforcement mechanism for CCPA, taking effect in 2023.

CCPA covers entities that meet any of the following:

- Handle data on over 100,000 California residents
- Has nexus and over $25 million in revenue
- Make over 50% of revenue from data transfer or sale personal data of California residents.
- Requires organizations to implement
- “Reasonable Security”

New Regulations for CCPA/CPRA Include:

- CPRA created the California Privacy Agency (which comes into action in 2023)
- Defined sensitive personal information to include social security number, driver’s license, account log-in, password, and even precise geolocation
- Contractor is defined as a service provider that can provide a “Certification” that it will, among other items, implement security safeguards

The Securities and Exchange Commission

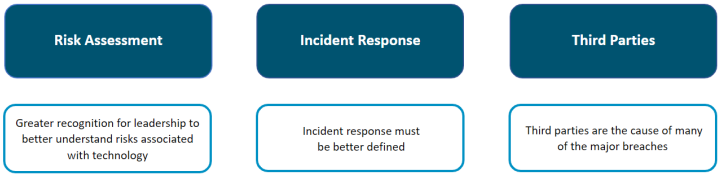
The SEC has shared guidance for boards on disclosing cybersecurity events and has more prescriptive guidance for financial firms. The SEC has broad jurisdiction, and their changes around cyber risk are aimed to be more rigid.

Potential Changes for Public Companies Include:

- Defined policies and procedures
- Clarity on managers role
- Board of Directors oversight and any expertise
- Updates to cyber incident details

There are also changes to regulated advisors that aim to be more stringent with an emphasis on third parties and risk assessment.

Three Common Themes Across Regulatory Changes



To address changes to NYS DFS, CCPA/CPRA, and SEC, key cyber areas must be evaluated and strengthened across organizations. These three themes include risk assessments, incident response, and third parties.

Risk Assessments

Many organizations say they’ve conducted a risk assessment, however what they really did was a gap analysis. Risk assessments must look at threats to the organization, the vulnerabilities in place, and the impact on the organization if threats act on vulnerabilities. It may be mapped to a framework, and it must include a clear prioritization of gaps. Paramount is that leadership across the organization, including the Board, is briefed on prioritized results from a risk assessment.

It is key to determine where threats could potentially infiltrate, then to build out priorities by understanding the gaps and vulnerabilities. It is also important to ask questions like do I have the right change

Risk assessments look at:

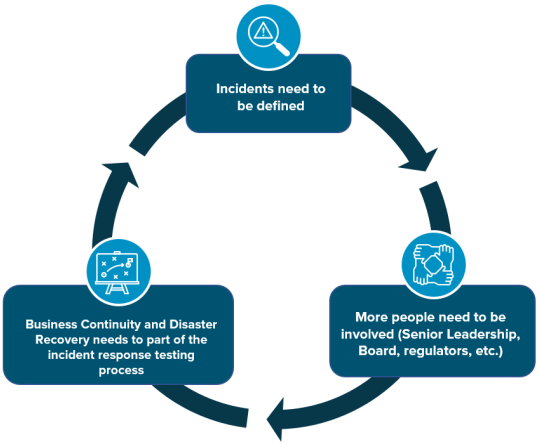


management? Are the right firewalls in place? Then bringing in a framework, preferably an industry standard like NIST, CIS or ISO, to map controls and determine where vulnerabilities exist. By using a publicly available framework, it is easier to translate across vendors and/or partners. It is vital to know the impact if a threat hits a vulnerability, for example - what happens when a phishing attempt works on a power admin with holistic access? If you know your vulnerabilities and which users have power admin rights, you can now prioritize this as a top focus area.

Regulators are pushing risk assessments so organizations know which vulnerabilities to address, and in what priority order to do so.

Incident Response

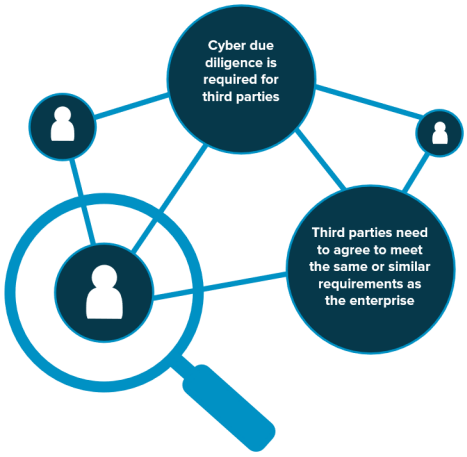
The definition of an incident must be clear and understood across the organization, including the Board. Intrusions or breaches are not incidents, so understanding what an incident means to your organization is crucial. There are different types of incidents each requiring different levels of response. Major incidents might involve the Board and require regulators to be notified, whereas minor incidents may only require internal remediation.



Business continuity and disaster recovery must be part of the incident response plan. Communication between these two units must be fluent and frequent. Incident response exercises and testing should include what would happen if a natural disaster were to occur and parts of organization are shut down. It is important to identify the team members involved on both sides and their individual and shared responsibilities.

Third Parties

To maintain compliance with regulatory changes, third party management must rely on thorough due diligence. Unfortunately, third parties are the cause of many major breaches, causing significant financial, operational, and reputational damage on organizations.



How you approach third party due diligence varies and there is no one size fits all, it may range from a straightforward questionnaire to an automated tool that assess risk using external objective data sources. It might be a mix of the two or something like contractual obligations, but either way due diligence must be put in place.

Your third parties must agree or meet similar requirements to those your organization has in place. You are responsible for customer and partner data, and if you share this data with third parties, they must be willing to meet the same or similar level of accordance.

Ramifications if something goes wrong at a third party reflect directly back on their partners and you may be just as liable. Cyber implications around third parties should be understood by senior leadership, the Board and any business units involved vendor decisioning and contracting. There are many different ways to approach this challenge, but you need to have a process, policy, and procedure understanding at all levels of the organization.

How K logix Helps

Keeping pace with changing regulations is achievable when focusing on key theme areas. We work with many security teams looking to bolster and evaluate their approach to risk assessments, incident response and third parties. Our approach is always white glove and focuses on meeting our customers where they are. If you are interested in learning more about our consulting services, let us know: info@klogixsecurity.com.

About the Author



Ryan Spelman has over 15 years of experience in homeland security and cybersecurity. He is currently K logix's Managing Director of Cyber Risk Consulting, focused on helping organizations navigate complex cyber risks. Ryan previously held leadership positions at Kroll, Center for Internet Security (CIS), and New York State Senate Committee on Veterans', Homeland Security and Military Affairs.

Image sources:

NYSDFS image source: https://www.dfs.ny.gov/

CCPA Image source: https://oag.ca.gov/privacy/ccpa

SEC image source: www.sec.gov