INSIGHTS

Cyber made simple.

one brightly cyber

CYBER REGULATIONS GROW STRICTER

BY JAY BORDEN

California and New York have rather strict cyber and privacy protocols for any business in the state or doing business with a citizen of the state. Both states are tightening their regulations and requirements to protect the privacy and information of users and citizens.

California's CCRA, California Privacy Rights Act of 2020 formed the CCPA, California Privacy Protection Authority. The CCPA was given the power to make regulations in order to enforce CCRA.

One of those regulations stated that any business collecting or processing the private information of consumer had to protect it and perform an annual cybersecurity audit. The intent of the audit is to determine what precautions are being taken in practice and the success of it in practice.

The new regulations now in the proposed stage tighten the requirements. Every company in performing the annual audit needs to:

- Detail each element in their cybersecurity program
- Looking at the program as a whole, identify any holes or weaknesses
- If a gap or weakness was found in a prior audit, explain the current state

If a company fails to include an element listed in the regulation, an explanation is required as to why it wasn't listed and why it isn't required in the company's protection of people's personal information. The company must provide how and why the safeguards in place meet the requirements of the regulations.

Using the Federal Trade Commission's requirements, each annual audit must "assess and document with specificity" the following:

- Multi-Factor Authentication
- Strong passwords
- Encryption of data
- Zero-trust architecture
- Privilege restrictions
- Secure configurations
- Patch mangement
- Logging of all events significant to security

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

CYBER REGULATIONS GROW STRICTER

Continued

It's important to remember that the logs must be tamper-proof and you must be able to prove it.

In order to document these and state their effectiveness, they must be in place. Basically, the CCPA is making them mandatory.

This change is in draft status now. But the direction of the CCPA is clear. Protection and cybersecurity are required, and you must be able to prove the requirements are being met.

The changes in New York proposed by Governor Kathy Hochul apply to hospitals.

When enacted, which is expected, hospitals have to become proactive in cyber defense, not just reactive. This requires the appointment of a CISO, Chief Information Security Officer, if one doesn't exist.

The proposed changes require creating and implementing:

- Multi-Factor Authentication, MFA
- Policies for determining and testing the security of each 3rd party application used by the hospital
- An incident response plan
- Testing of the Incident Response Plan to show that patient care can be delivered during a cyber event

Governor Hochul said "Our interconnected world demands an interconnected defense against cyber-attacks, leveraging every resource available, especially at hospitals,"

"These new proposed regulations set forth a nation-leading blueprint to ensure New York State stands ready and resilient in the face of cyber threats." Hospitals have been required to conform to HIPAA which is less prescriptive by design. The Governor's proposed changes complement HIPAA, not replace it.

As with California, the need and oversight of cybersecurity is becoming more tightly defined and overseen.

Is your company ready to meet these requirements? We can help.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920