What do Nevada, New York, South Carolina, and Vermont have in common?

Date : 07-06-2018

They are early adopters in moving cyber governance toward mainstream awareness in corporate boardrooms. This year we've seen the European Union enact the GDPR, US and EU regulators question Facebook for their handling of user data, and the SEC release guidelines for appropriate responses to data breaches. Several states, including NV, NY, SC, and VT have passed (or have pending) legislation requiring the financial services industry maintain stricter compliance, diligence, and disclosure standards regarding cyber risks.

South Carolina's Insurance Data Security Act enforces the following requirements for insurance providers:

- To investigate and report a cybersecurity event
- To implement a comprehensive cybersecurity program based upon risk assessment
- To conduct due diligence on third-party service providers
- To certify compliance with the Act

The cyber legislation across NV, NY, SC, and VT has a similar goal: increase trust and transparency. We can expect similar legislation to affect many different industries. If your firm collects or stores personal information about customers or suppliers, your business is likely to face these requirements.

A good *Cyber Blueprint* requires boards monitor externalities such as pending cyber legislation affecting other industries. Is your board's risk committee focused on this issue? Has your board evaluated the establishment of a technology or cybersecurity subcommittee?

The process doesn't need to cost millions or require an army of consultants. It takes focus, experience, and a commitment to demonstrate leadership for your customers, suppliers, employees, and investors.

- Jim Pflaging