Connecticut Senate Weighs New Requirements for Large-Scale Data Breaches: 4 Ways to Prepare

Insights
2.23.26

Connecticut-based companies that fall victim to large-scale data breaches could face a new slate of disclosure and investigation requirements under legislation currently being considered in the state. Connecticut State Senate Bill 117 (SB00117), *An Act Concerning Breaches of Security Involving Electronic Personal Information*, would create a new category of "massive" cyber incidents. If passed, organizations that experience such a breach will have to hire a third-party investigator and provide the results of the investigator's report to the state attorneys general, or face penalties. Organizations in other jurisdictions should prepare for what could likely be a cascade of similar regulations given the propensity of states to "one-up" each other in this domain. This Insight provides an overview of the most salient provisions of the bill and what your business can do to best prepare.

What Would the Bill Do?

SB00117, which is currently pending before the Connecticut senate, seeks to establish new requirements following "massive" cyber security attacks. The bill would define a "massive breach of security" as where:

- the personal information of at least 100,000 residents of Connecticut have been breached or is reasonably believed to have been breached, and
- the breach of security occurred due to the unauthorized use of a computer or computer network.

New Mitigation Requirements

If enacted, organizations that face cyberattacks that meet this definition would have to take mandatory steps to address the breach, including:

(1) Mandatory Third-Party Forensic Investigations: the law would require impacted businesses to retain a third-party forensic investigator to prepare a detailed forensic report disclosing:

- the results of the forensic investigation and analysis, and

- "how the unauthorized use that gave rise to the massive breach of security occurred, as well as the root causes of such unauthorized use."

While many victims elect to retain a forensic investigation firm following a breach, Connecticut's proposed legislation would **mandate** what is currently elective. Keep in mind, SB00117 imposes the cost of a forensic investigation on the victim of the attack.

(2) Mandatory 90-Day Disclosure of the Forensic Report's Findings to the AG: the forensic report compiled by the third-party investigator (see above) must be submitted to the AG "not later than ninety days following the discovery of the massive breach of security," under the pending legislation.

It's important to note the bill explicitly states that "all forensic reports provided to the Attorney General…shall be exempt from public disclosure," alleviating the concern that a report's findings could be subject to Freedom of Information Act requests. But, the bill does permit the AG to "make such…forensic reports available to third parties in furtherance of [an] investigation," which raises a host of issues concerning attorney-client privilege.

AG's Ability to Recover Your Fumble

Importantly, if an organization fails to initiate a third-party investigation and submit a report within the mandated timeframe, the proposed legislation would permit the state AG to retain their own third party to "perform a forensic examination and analysis."

While larger organizations may have the bandwidth to handle a data breach while overseeing a complex forensic investigation, smaller entities would not be able to cite a "lack of resources" to sidestep the requirement.

Serious Fines for Noncompliance

Under SB00117, failure to submit the third-party report into a "massive" breach can result in civil penalties of $100,000 for small businesses and $500,000 for regular-sized entities. Don't forget, most insurance policies typically do not cover fines or penalties, as insuring against punishment is generally considered to be contrary to public policy.

Key Takeaways For Employers

As states like Connecticut consider setting new requirements for organizations to address cyber security incidents, there's several ways you can stay ahead of the curve and in compliance.

What can your organization do to prepare for engaging a third-party forensic investigator?

- Determine if your cyber insurance covers the costs of a forensic investigation. If you don't currently have cyber insurance, or your existing plan doesn't provide this coverage, consider

alternatives.

- Explore whether entering into a retainer arrangement with a forensic investigator would lower the fee in the event an investigation is required.
- Consult with legal counsel for their provider recommendations. Attorneys regularly work with forensic firms and can advise on which are best suited for your business.

What can your organization do to avoid punitive fines and other civil sanctions?

- Comply with the law. Have a plan in place to address each requirement to keep you on track.
- Retain counsel with expertise in data protection and cybersecurity who can help navigate the legal complexities of statutes and regulations.
- Prepare in advance. The more details you have worked out before a breach, the less likely you will make a mistake, or encounter delays during your response.

How can your organization avoid the AG taking over a forensic investigation?

- Designate which forensic firm you're going to retain from the outset and have a Master Services Agreement in place. Avoiding the need to hammer out legal details expedites the process.
- Know how you're going to pay for their service. Whether this expense is covered by your cyber insurance policy, or you've set aside funds, having the ability to cover the cost of a forensic investigation is essential.
- Keep your attorneys closely involved to ensure that the forensic investigator is satisfying legal requirements within the allotted time.

How can your business preserve the maximum amount of confidential information?

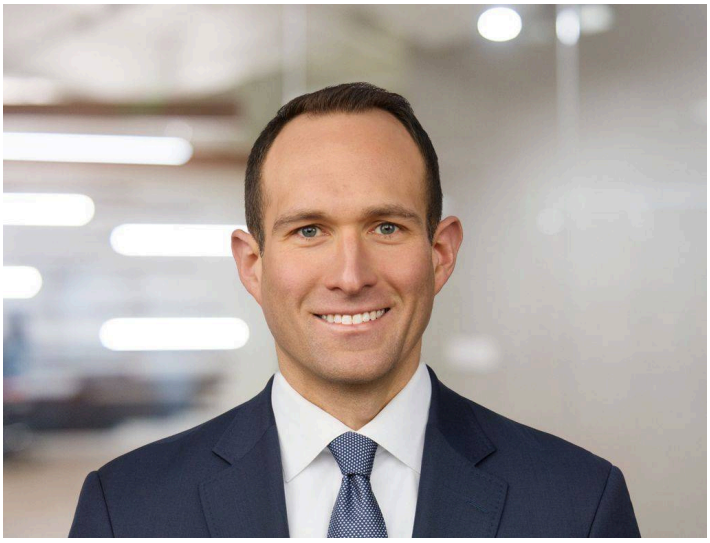
- Retain legal counsel immediately upon discovering a breach, and ensure that all communication, including that with the forensic investigation firm, is conducted through your attorneys.
- Review and consider upgrading your cybersecurity capabilities. The smaller the gap between your organization and industry standards, the less room regulators will have to find fault with your cybersecurity posture.
- Develop a proactive playbook for how you will work with a forensic investigator. Navigating a cyber incident is difficult, and the 90-day ticking clock in the background only adds more pressure on your company.

Conclusion

Fisher Phillips will continue to monitor developments and provide updates as warranted, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information

direct to your inbox. If you have questions, please contact your Fisher Phillips attorney, the authors of this Insight, or any member of our Data Protection and Cybersecurity Team.

Related People



Logan S. Booth, CIPP/US
Of Counsel
720.644.2889
Email

Daniel Pepper, CIPP/US
Partner
303.218.3661
Email

Service Focus

Privacy and Cyber

Data Protection and Cybersecurity

Trending