BURR FORMAN LLP

"Figuring Out the Details: Practical Tips for Evaluating and Investigating Cyber Incidents and Claims" CLM Magazine

Firm News
10.21.2022

For the October 2022 issue of CLM Magazine, published by the Claims and Litigation Management Alliance, Robert Given authored an article laying out practical tips for claims professionals to evaluate and investigate claims related to cybersecurity incidents.

In addition to immediately identifying any applicable policies and their coverages upon an insured's reporting of an incident, insurers should be sure the insured has the resources in place to effectively respond to the incident as required by state and federal law and any applicable cyber policy. At a minimum, the insured should immediately:

- Retain approved legal counsel;
- Engage with forensic examiners and its breach-response team;
- Determine whether reporting to law enforcement is appropriate; and
- Determine any state and federal notification requirements.

It is also important to identify the initial costs and damages, which can entail PR and crisis management expenses, business interruption loss, system monitoring expenses, cyber extortion loss and data recovery loss. From there, the insurer needs to learn more about the nature of the incident, especially noting that additional challenges and costs occur if the incident affects a third-party, including risk of civil and criminal regulatory penalties. The most likely source of regulatory liability stems from potential failure to meet reporting requirements, and some considerations to mitigate

RELATED PROFESSIONALS

Robert S. Given

RELATED CAPABILITIES

Cybersecurity & Data Privacy

"Figuring Out the Details: Practical Tips for Evaluating and Investigating Cyber Incidents and Claims" CLM Magazine

risk include:

- States can impose their own requirements, and those operate independently of each other and federal requirements. The locations of the affected individuals must be determined for the insurer to evaluate the damages.
- Federal law imposes reporting and notice requirements that apply based on who the target of the breach was. For example, following most breaches, financial institutions must meet the reporting requirements of the Gramm–Leach–Bliley Act. And HIPPA imposes on covered providers different reporting obligations for breaches involving protected health information.[1]
- Federal requirements can also change based on the type of data or information compromised.

As for investigating third-party liability, Given offered the following steps to cast a wide net:

- Identify, if possible, the likely responsible parties;
- Identify the possible risks for misuse of the particular personal information and data compromised;
- Identify all parties involved in maintaining or operating the breached system;
- Determine key features of the breached system's security:
- Whether the insured's provider(s) manages the system through remote access credentials, which are particularly vulnerable to cyber attack;
- Whether the insured's provider(s) selected and installed the anti-virus software for the system;
- Whether the insured's provider(s) was responsible for updating and installing patches for any of the insured's computer programs;
- Whether the insured's provider(s) established firewall rules for the insured's system;
- Whether the insured's provider(s) was responsible for monitoring for suspicious activity; and
- Whether the insured's provider(s) was responsible for any part of the insured's network design — *g.*, segregation, or lack thereof, of network areas containing sensitive or confidential information.
- Determine whether one or more parties' conduct in the lead up to the breach deviated from established procedures or courses of dealings related to the compromised system.

For the full article, please click here.

[1] Note that on March 15, 2022, President Biden signed into law significant new federal data-breach legislation requiring all organizations in critical infrastructure sectors to report cyber incidents to the Department of Homeland Security within 72 hours. In the coming months and years, federal administrative rules will expand and clarify which organizations are covered and what those organization's post-breach obligations are.