#ForensicPerspectives

Regulatory expectations after a data breach

The US Securities and Exchange Commission has outlined guidance for registrants, including:

Financial impact

If your company has a material breach, the financial impact must be disclosed in a timely manner while complying with Regulation FD and selective disclosure obligations. In addition, the costs of investigating and responding need to be accrued in a timely manner. Companies also have a continuing duty to update or correct, as appropriate.

Preparedness

If your company does not have adequate processes in place to prevent, detect, disclose, and/or correct a breach in a timely manner, that may need to be disclosed.

Insider trading

If your leadership trades securities while in possession of material non-public breach-related information, the SEC may consider it unlawful insider trading.

Board oversight

Ensure that your board is engaged in the oversight of cyber risks and incidents, and that you can evidence such, if necessary.

Portfolio impact

Ensure that your board is engaged in the oversight of cyber risks and incidents, and that you can evidence such, if necessary.

Mergers impact

If a target company is acquired through the purchase or sale of securities, and if a material cyber incident occurred pre-close and was not disclosed to the purchaser, then the SEC may consider this to be securities fraud.

Other regulators and governmental entities have also communicated various expectations, and in some cases the penalties for non-compliance are severe, including potential criminal exposure.

Kristofer Swanson, CPA/CFF, CFE, CAMS | Vice President & Practice Leader, Forensic Services
+1-312-619-3313 | kswanson@crai.com