#ForensicPerspectives

Cyber insurance claims: **What companies need to know**

Be prepared

Be prepared for a cyber event before it happens: identify applicable policies; know what documentation and information will be necessary; confirm that key legal, technology and finance personnel understand their roles; and create and maintain process documentation.

Track your costs

Companies incur a lot of costs after a cyber event – begin tracking them immediately. Tracking costs in real time enables companies to more efficiently and effectively prepare insurance claims.

Know what costs are covered

Companies often improve their security after a cyber event, but the cost of improvement is not usually covered. Find out what services are covered by your policy and either contract covered services separately or have vendors itemize costs to allow for an analysis of covered versus non-covered services.

Understand your reporting obligations

Understand all potential policies at issue, when to notify the insurers, when to seek approval for vendors, and when to file a proof of loss – or seek an extension.

Explain your claims

Provide written explanations of the description of services and the basis for the claim to eliminate the time it takes insurers to review, process, and pay claims. Providing copies of invoices will likely not be fully sufficient.

Business interruption losses

Measure lost profits resulting from the covered event and make sure to consider other implications that might be impacting the analysis, including prevailing market conditions, possible delayed sales, capacity constraints, seasonality, avoided expenses, and extra expenses.

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