expel

FAST FACTS SHEET

The new Securities and Exchange Commission (SEC) public company cybersecurity disclosures

New SEC cybersecurity regulation changes were published in December 2023, and they're here to stay. With a ton of details to absorb and zero tolerance for getting it wrong, here's what it is, action items for compliance, and how Expel can help.

What's the new regulation?

As of December 15, 2023, public (and aspiring public) companies have to report material cybersecurity incidents to the SEC within four business days of determining they're material.

Plus, the SEC wants all the details on your cybersecurity risk program processes, involvement of assessors or consultants, and policies for third-party service providers.

What do I need to do to comply, and how can Expel help me?

1. **Identify when you need to report incident activity to the SEC, and determine if an incident can be considered material.** Expel can help you report on what matters (to you and the SEC) with our built-in severities rating, and assist you in defining and tracking what's critical.

So, what's considered material?

The short answer is...it depends. The SEC cybersecurity rules describe a material incident as a matter **"to which there is a substantial likelihood that a reasonable investor would attach importance"** in an investment decision.

There is not a specific financial threshold for a material cyber incident. In fact, the SEC states in the regulation, **"...some cybersecurity incidents may be material yet not cross a particular financial threshold."**

TL;DR - For all the nitty-gritty legal stuff, check out this **handy SEC resource.**

2. **Get answers fast.** Reporting speed is a key part of this requirement, and four days isn't a ton of time. Expel can automate critical actions (ingestion, log analysis, detection, and correlation) and help your analysts understand root causes quickly via our SecOps platform, Expel Workbench™. Plus, we constantly monitor your environment through our superior MDR services, spanning all attack vectors (from on-prem to Kubernetes).

3. **Perform root-cause analyses quickly, and use this information to build resilience.** Expel can help answer the who, what, where, when, and how so you understand what happened, and how you can improve.

4. **Produce incident reports that use simple language and can inform a variety of audiences from the SEC to board members.** By default, Expel generates reports that show our work and are easy to understand, with or without a technical background.

While new compliance regulations can sound intimidating, none of these requirements are challenges for Expel.

Additional help from Expel

Expel MDR provides superior execution, accuracy, and speed compared to anyone else in the market, and is supported by our SecOps platform, **Expel Workbench**™. With Expel, you get:

- **World-class threat detection and intelligence** that provide proactive, actionable insights
- **24x7x365 SOC monitoring** for your cybersecurity infrastructure, no matter how complex it is
- **Automate critical actions** including ingestion, log analysis, detection, and correlation