FAST FACTS SHEET

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

Changes in SEC regs are coming into effect before EOY 2023, with a ton of details to absorb and zero tolerance for getting it wrong.

Here's what it is, an overview of what you need to do, and how Expel delivers answers—fast.

What's the new regulation?

Starting December 18, 2023, public (and aspiring public) companies have to spill the beans on SEC-mandated cybersecurity deets, like reporting incidents ***within four business days of determining they're material.***

Plus, the SEC wants all the details on your processes for your cybersecurity risk program, 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 new 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 MDR and threat hunting offerings, spanning across attack vectors (from on-prem to Kubernetes).

3. **Perform root-cause analysis and quickly organize the information and context needed for incident disclosure to the SEC, *and* use this info 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. **Generate reports that explain incidents in language that's easy to understand and can be used as the basis of reports to a variety of stakeholders, such as the SEC, board members, and stakeholders.** Expel can help by showing our work in language that's easy to understand, with or without a technical or InfoSec background.

Did you know?

While new compliance regulations can sound intimidating, none of these requirements are new challenges for Expel, because we always operate with **transparency and speed.**

Feeling overwhelmed? Expel is built by experts with global visibility across hundreds of customers and industries, and we're here to answer your questions and provide the context you need to work with the SEC (yes, in just four days), while continuing to build resilience.

Additional help from Expel

Expel MDR and Expel Threat Hunting:

- Provide many of the necessary details for incident disclosure
- Satisfy the risk management and governance components of the disclosure rules
- Remove attackers from your organization's infrastructure

And Expel Threat Hunting can help identify the next areas of potential attack. That's a win-win-win-win.

86AYNER2Z-12/15/23