KnowBe4

KnowBe4's Guidance on the SEC New Rule Requiring Firms to Disclose Cybersecurity Breaches

James McQuiggan, KnowBe4 Security Awareness Advocate

***Quoted:** SecurityWeek, The Hacker News, Security Boulevard, eSecurityPlanet, The Cybersecurity News, and Wired Focus*

"***The new requirement set forth by the SEC requiring organizations to report cyber attacks or incidents within four days while seeming aggressive sits in a more lax time frame than other countries.***

Within the EU, the UK, Canada, South Africa, and Australia, they all have 72 hours to report a cyber incident. In other countries like China and Singapore, it is 24 hours. India has to report the breach within six hours.

Either way, organizations should have repeatable and well-documented incident response plans with communication plans, procedures, and requirements on who is brought into the incident and when. Part of this documentation will need to involve when to inform the SEC if they are publicly traded.

Organizations must stay current on local cybersecurity laws and regulations to ensure compliance and foster a prompt incident reporting and response culture."

Brian Jack, KnowBe4 CISO

"This is nothing new. There are existing regulations and laws such as HIPAA, GDPR, and almost every state in the U.S. that requires a notification to be made when a breach of certain data types occurs. Many of these laws and regulations require an organization to provide notice without undue delay while others are more prescriptive, the shortest time frame being 72 hours for GDPR-based breaches. You may also have separate commercial contracts with customers or vendors that outline a stricter notice time when certain cyber events happen.

Every incident response and breach response plan should include what, when, and to whom you will make a breach notification. It should be practiced at least annually as part of table top simulations for incident response. An organization should take an inventory of any prescriptive regulations or laws that they are subject to, and ensure that they are prepared to make the required notices to the correct authorities if a cyber breach event should happen.

The final thing I will note is that if an organization holds cyber liability or other breach liability insurance, they must discuss the proper process for handling breaches with the insurance company and ensure they contact only covered breach response vendors. This is very important and often overlooked since not following the terms of the insurance policy can cause your entire claim to be denied and your organization to have no insurance based assistance. Most cyber liability coverage will include legal assistance with a breach and part of that is navigating when you need to make certain disclosures."

© 2023 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.

KnowBe4's Guidance on the SEC New Rule Requiring Firms to Disclose Cybersecurity Breaches

Roger Grimes, KnowBe4's Data Driven Defense Evangelist

"This is not an issue we should respond lightly to. It is a vast legal issue with all sorts of ramifications that will impact every public corporation evermore. With that said, a few notable points:

- You do not have to report a cybersecurity incident until you determine its "material". Materiality is a legal term used in GAAP...meaning you do not have to report until you think that it is impactful enough that normal financial statement readers would care. In practice, it is often meant it does not have to be reported unless it impacts revenues something like 10% (but it is not a hardcoded amount). That is a HUGE amount and in many cases, that means many companies will not report.
- The four-day rule actually applies to materiality, meaning you do not have to report until four days AFTER DETERMINING materiality. So if it takes you months to determine if the cybersecurity incident is material, it takes months.
- The far bigger impact is the SEC now telling BoDs that the BoD must prove they understand cybersecurity risk. THIS IS HUGE! It is going to change our field. Billions will be spent from here on to meet the requirements outlined in this rule. This rule will have far more impact than the four-day rule.
- Regarding four days, GDPR is three days and India has a six-hour rule.
- There are many "outs" on our four-day rule...enough so that if you want a wormhole, you will probably find one."

© 2023 KnowBe4, Inc. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.