What Organizations Need to Know About New

SEC Data Breach Reporting Requirements

Newly introduced SEC reporting requirements now compel publicly traded companies to report "material" cybersecurity incidents within four business days and outline related details on risk management and strategy in their 10K filings.

These new requirements are just one of many indications that governments are taking more public action when it comes to protecting data. Companies are now beginning to understand that the evaluation of their preparation and response may have as much reputational impact as the data breach itself.

Adding to the complexity is the quickly evolving regulatory environment in the U.S. that is likely to see further changes and court challenges in the wake of recent Supreme Court decisions.

With this increased SEC scrutiny, companies now need to up their game and will have to consider:

Beyond whether they have a response plan or not. Today, the quality of that response plan is even more critical.

This escalates the need to modernize the approach to response plans – from crisis planning to investor relations. As quickly as the threat landscape is evolving and organizations themselves change, clients will need to make sure their response plans have adapted as well.

How (or if) their plan was rehearsed and reinforced through employee training.

Immersive and effective table-top training sessions and simulations help practice established plans. To further increase effectiveness, it's important to plan and execute creative and engaging employee training campaigns that ladder to those plans and priorities as well.

Public disclosure requirements in response to a data breach can represent just the beginning of the reputational risk companies face due to government regulations or actions following a data breach:

Disclosing a breach that's had a material impact on business can lead to subsequent action by government entities – and already has in many cases. Such actions include public investigations and legislative hearings, presenting far greater reputational risk than the initial disclosure.

As governments face more pressure to act against cybercriminals and protect the data of their citizens, they are also taking additional – and more public – steps to hold companies that are compromised by data breaches accountable.

FLEISHMANHILLARD