With the proliferation of cybercrime and recently proposed legislations related to cyber risk reporting and disclosures, organizations are under intense pressure from stakeholders to respond to inquiries about the effectiveness of their cyber risk management programs. The pressure is compounded by the reality that there is no single approach for reporting on such programs and related controls.

During an October 27 Dbriefs webcast, Deloitte surveyed over 3,400 professionals to gain insights into their views on cyber risk management oversight and reporting. Here’s what they had to say.

What do you believe is the biggest challenge associated with cybersecurity at your organization?

- Technology innovation: 13.4%
- Poorly designed/antiquated technology: 8.5%
- A focus on compliance, not security: 16.4%
- Data growth: 17.4%
- Failure to implement security fundamentals: 25.3%
- Other: 25.0%

19% responded “Don’t know or N/A,” based on 2,573 responses received.

Even with significant investments being made, it is difficult for organizations to fully protect against cybersecurity attacks and breaches. Results of the polling support the reality that there is no single or unified approach for performing and reporting on an organization’s cyber risk management program and related controls.

Stakeholders can benefit from a cybersecurity risk management examination engagement by having a standardized reporting mechanism, providing a broad range of users with useful information to support informed decision making.

The time to act is now by investing in a readiness assessment in order to prepare and ready management for a future independent third-party cybersecurity risk management examination engagement.