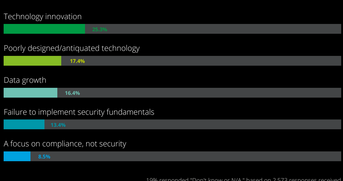
The cybersecurity examination
Raising the bar for cyber risk management oversight and reporting

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?



19% responded "Don't know or N/A," based on 2,573 responses received

Total spent on Cyber Security in 2015[1]
$75.4 Billion

Number of data breaches reported in 2015[2]
2,122 Breaches

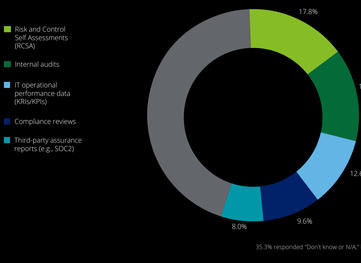
Number of records breached in 2015[2]
700 Million

Estimated yearly total cost from breaches[2,3]
~$107 Billion

Average time to detect a breach[3]
~6.5 Months

Even with significant investments being made, it is difficult for organizations to fully protect against cybersecurity attacks and breaches.

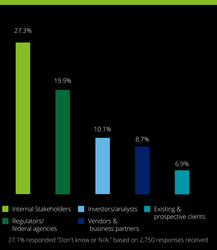
Which cyber risk monitoring and reporting mechanisms does your company utilize and rely on today?



35.3% responded "Don't know or N/A," based on 2,859 responses received

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.

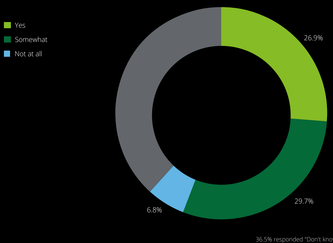
Today, which stakeholder group typically requests the most information about your entity's cybersecurity risk management program to support informed decision making?



27.1% responded "Don't know or N/A," based on 2,750 responses received

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.

Does your organization perceive value in having an independent, single reporting mechanism for questions related to an entity's cybersecurity risk management program?



36.5% responded "Don't know or N/A," based on 2,528 responses received

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.

"How did you react to these results? Share your opinion with @DeloitteRisks."

Deloitte.

[1] "Gartner Worldwide IT Spending Forecast," Gartner
[2] "2015 Data Breach Investigations Report," Verizon
[3] "2015 Cost of Data Breach Study: Global Analysis," Ponemon and IBM