Fear of cyber attacks, data breaches could expose enterprises to emerging security risks: Gartner

TEXT SIZE
2013-11-11

Fear, uncertainty and doubt over the possibility of cyber attacks and data breaches may be producing greater security risks as organizations veer away from tried-and-true, risk-based tactics, notes a new survey from Gartner Inc.

That fear is causing security professionals to shift focus away from disciplines such as enterprise risk management and risk-based information security to technical security, suggests the Gartner 2013 Global Risk Management Survey.

The survey – which involved a total of 555 organizations in the United States, Canada, the United Kingdom and Germany – was addressed to employees who are responsible for privacy, IT risk management, information security, business continuity or regulatory compliance, notes a statement from Gartner, an information technology research and advisory company.

Gartner analysts suggest that fear, uncertainty and doubt (FUD), which often leads to reactionary and highly emotional decision-making, is driving the change.

"While the shift to strengthening technical security controls is not surprising given the hype around cyber attacks and data security breaches, strong risk-based disciplines such as enterprise risk management or risk-based information security are rooted in proactive, data-driven decision making," John Wheeler, research director at Gartner, says in the statement. "These disciplines

focus squarely on the uncertainty (as in, risk), as well as the methods or controls to reduce it. By doing so, the associated fear and doubt are subsequently eliminated," Wheeler continues.

Only 6% of those taking part in the survey focused on enterprise risk management in 2013 compared to 12% in 2012.

As IT risk profiles and postures change in the future, an inevitable shift in focus back to these risk-based disciplines will need to occur, Wheeler argues. If that does not take place, IT organizations may find that more-critical, emerging risks will remain undetected, and the company as a whole will be left unprepared, the Gartner statement adds.

In addition, this year's survey shows that 53% of respondents reported using either informal IT risk management steering committees or none at all compared to 39% of respondents in 2012.

While FUD can lead to negative management behaviours, Gartner points out, it can also produce positive budget impacts for an IT risk management program. In the short term, this can be a benefit by affording the ability to add staff and resources to an area that is typically cost-constrained.

Consider that 39% of respondents in 2013 have been allocated funds totalling more than 7% of the total IT budget, Gartner reports. That is up significantly from the 23% of respondents who received a similar amount in 2011.

That added budget resource, however, is not necessarily a given going forward. "Unless there is a strong IT risk management program in place to support the future need for similar levels of budget allocation, the resources will soon evaporate," Gartner adds.

The company recommends that chief information officers, chief information security officers, and senior business executives assess the current maturity of their IT risk management program, and create a strategic road map for risk management to ensure continued funding.

Wheeler further suggests that regular communication about emerging IT risks with board members and business leaders will result in better decision-making and, ultimately, more desirable business outcomes.

Source: http://www.canadianunderwriter.ca/news/fear-of-cyber-attacks-data-breaches-could-expose-enterprises-to-emerging-security-risks-gartner/1002715690/q7lw4rW0uuy843rlrq4xrM2vx/?ref=enews_CU&utm_source=CU&utm_medium=email&utm_campaign=CU-EN11122013