Gartner

Press Release

CONTACTS:
Janessa Rivera
Gartner
+ 1 408 709 8220
janessa.rivera@gartner.com

Robert van der Meulen
Gartner
+ 44 (0) 1784 267 738
rob.vandermeulen@gartner.com

Gartner Survey Finds That Fear of Cyberattacks and Data Breaches Could Leave Organisations Exposed to Emerging Security Risks

Fear of Attacks is Shifting Focus From Tried and True Risk-based Tactics

STAMFORD, Conn., November 7, 2013 — Recent publicity about cyberattacks and data security breaches has increased IT risk awareness among CIOs, chief information security officers (CISOs) and senior business executives. However, Gartner, Inc.'s 2013 Global Risk Management Survey found that fear of attack is causing security professionals to shift focus away from disciplines such as enterprise risk management and risk-based information security to technical security. This shift in focus is driven by what Gartner analysts refer to as fear, uncertainty and doubt (FUD), which often leads to reactionary and highly emotional decision making.

"While the shift to strengthening technical security controls is not surprising given the hype around cyberattacks 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," said John A. Wheeler, research director at Gartner. "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."

IT risk management programs and approaches differ by industry and by company, according to the unique business needs and requirements that an IT organisation must support. Gartner views the spectrum of IT risk management programme activities enabling one or more of the following five functions:

1. Technical security
2. Risk-based information security
3. IT operations risk — formalised risk management across multiple disciplines, such as security, privacy, business continuity management (BCM) and compliance
4. Operational risk — IT operations risk plus business operational risk, supply chain risk and more
5. Enterprise risk management — operational, credit and market-risk-centralised function with executive and board-level visibility

Gartner said that organizations that either shift away from risk-based disciplines or simply fail to adopt them will find themselves at the mercy of the FUD trap. The survey results showed movement away from these disciplines, with only 6 per cent focused on enterprise risk management in 2013 versus 12 per cent in 2012. Mr Wheeler said that 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. If not, IT organisations may find that more-critical, emerging risks will remain undetected, and the company as a whole will be left unprepared.

While FUD can lead to negative management behaviours, it can also lead to positive budget impacts for an IT risk management program. In the short term, this can be a benefit to the programme through the ability to add staff and resources to an area that is typically cost-constrained. In fact, 39 per cent of this year's survey respondents have been allocated funds totalling more than seven percent of the total IT budget. That compares with only 23 per cent of survey respondents receiving a similar amount in 2011.

However, the added budget resources are not a given for future years. Unless there is a strong IT risk management programme in place to support the future need for similar levels of budget allocation, the resources will soon evaporate. Determining the IT risk management programme's current level of maturity, as well as the desired state of maturity, is a great first step to building a strong programme. Gartner recommends that CIOs, CISOs and senior business executives assess the current maturity of their IT risk management programme, and create a strategic road map for risk management to ensure continued funding.

At the management levels, IT risk management governance is weakening. Compared with Gartner's 2012 survey results on the use of IT risk management steering committees, many companies are shifting away from formal risk management governance structures. Overall, in 2013, 53 per cent of survey participants reported using either informal IT risk management steering committees or none at all. This compares with 39 per cent in 2012.

"These incongruent survey findings seem to validate the observation that risk-based, data-driven approaches are falling to the wayside in favour of FUD-based, emotion-driven activities," said Mr Wheeler. "Or, perhaps more disturbingly, they indicate that those who have concerns are simply burying their head in the sand, rather than proactively addressing emerging threats."

Mr Wheeler said 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.

Survey participants also indicated that progress is slowing to link IT risk indicators and corporate performance indicators. Not only did activity supporting the formal mapping of key risk indicators (KRIs) to key performance indicators (KPIs) decline by 7 per cent from 2012 to 2013, but mapping also ceased altogether for 17 per cent of survey respondents in 2013, versus 8 per cent in 2012. Again, this shift in activity could very well be a result of the FUD-based, emotion-driven approaches.

"If done correctly, integrated risk and performance mapping exercises can yield tremendous benefits for companies and IT organisations that are seeking to develop a more-effective risk management dialogue with business leaders," said Mr Wheeler. "However, if done incorrectly, the exercise can become time and resource consuming, often resulting in an unwieldy process that ultimately fails."

Additional information is available in the report "Survey Analysis: Risk Management, 2013." The report can be found on Gartner's web site at www.gartner.com/resId=2606115.

About the Gartner 2013 Global Risk Management Survey
The Gartner 2013 Global Risk Management Survey was addressed to employees who are responsible for privacy, IT risk management, information security, business continuity or regulatory compliance. Gartner surveyed a total of 555 organisations in the US, Canada, the UK, and Germany in April and May 2013 to help understand how risk management planning, operations, budgeting and buying are performed, especially in areas such as risk management, information security, business continuity management, IT compliance and privacy.

About Gartner
Gartner, Inc. (NYSE: IT) is the world's leading information technology research and advisory company. Gartner delivers the technology-related insight necessary for its clients to make the right decisions, every day. From CIOs and senior IT leaders in corporations and government agencies, to business leaders in

high-tech and telecom enterprises and professional services firms, to technology investors, Gartner is a valuable partner in more than 13,000 distinct organizations. Through the resources of Gartner Research, Gartner Executive Programs, Gartner Consulting and Gartner Events, Gartner works with every client to research, analyze and interpret the business of IT within the context of their individual role. Founded in 1979, Gartner is headquartered in Stamford, Connecticut, USA, and has 5,800 associates, including more than 1,450 research analysts and consultants, and clients in 85 countries. For more information, visit www.gartner.com.

# # #