Gartner | Press Release

Media Contacts
Susan Moore
Gartner
Tel. +61 2 9459 4692
susan.moore@gartner.com

Laurence Goasduff
Gartner
+44 1784 267 195
laurence.goasduff@gartner.com

Gartner Says Monitoring Employee Behaviour in Digital Environments is Rising

Latest Security Trends Will Be Explored at Upcoming Gartner Security & Risk Management Summits 2012 in Maryland, Sydney and London

Sydney, 29 May 2012 — Monitoring employee behaviour in digital environments is on the rise, with 60 per cent of corporations expected to implement formal programs for monitoring external social media for security breaches and incidents by 2015, according to Gartner, Inc. Many organisations already engage in social media monitoring as part of brand management and marketing, but less than 10 per cent of organisations currently use these same techniques as part of their security monitoring programme.

“The growth in monitoring employee behaviour in digital environments is increasingly enabled by new technology and services,” said Andrew Walls, research vice president of Gartner. “Surveillance of individuals, however, can both mitigate and create risk, which must be managed carefully to comply with ethical and legal standards.”

To prevent, detect and remediate security incidents, IT security organisations have traditionally focused attention on the monitoring of internal infrastructure. The impact of IT consumerisation, cloud services and social media renders this traditional approach inadequate for guiding decisions regarding the security of enterprise information and work processes.

“Security monitoring and surveillance must follow enterprise information assets and work processes into whichever technical environments are used by employees to execute work,” said Mr Walls. “Given that employees with legitimate access to enterprise information assets are involved in most security violations, security monitoring must focus on employee actions and behaviour wherever the employees pursue business-related interactions on digital systems. In other words, the development of effective security intelligence and control depends on the ability to capture and analyse user actions that take place inside and outside of the enterprise IT environment.”

The popularity of consumer cloud services, such as Facebook, YouTube and LinkedIn, provides new targets for security monitoring, but surveillance of user activity in these services generates additional ethical and legal risks. There are times when the information available can assist in risk mitigation for an organisation, such as employees posting videos of inappropriate activities within corporate facilities. However, there are other times when accessing the information can generate serious liabilities, such as a manager reviewing an employee's Facebook profile to determine the employee's religion or sexual orientation in violation of equal employment opportunity and privacy regulations.

“The conflicts involved were highlighted through recent examples of a small number of organisations requesting Facebook login information from job candidates,” said Mr Walls. “Although that particular practice will gradually fade, employers will continue to pursue greater visibility of social media conversations held by employees, customers and the general public when the topics are of interest to the corporation.”

A wide range of products and services have emerged to support these actions and many PR organisations provide social media monitoring as a standard client service. Security organisations are

-more-

beginning to see value in the capture and analysis of social media content, not just for internal security surveillance, but also to enable detection of shifting threats that impinge on the organisation. This might be physical threats to facilities and personnel revealed through postings concerning civil unrest or it may be threats of logical attacks by hacktivists. Early detection of shifting risks enables the organisation to vary its security posture to match and minimise negative impacts.

“The problem lies in the ability of surveillance tools and methods to produce large volumes of irrelevant information,” said Mr Walls. “This personal information can be exposed accidentally or become the target of voyeuristic behaviour by security staff.”

There are a number of important issues that also need to be considered. While automated, covert monitoring of computer use by staff suspected of serious policy violations can produce hard evidence of inappropriate or illegal behaviours, and guide management response, it might also violate privacy laws. In addition, user awareness of focused monitoring can be a deterrent for illicit behaviour, but surveillance activities may be seen as a violation of legislation, regulations, policies or cultural expectations. There are also various laws in multiple countries that restrict the legality of interception of communications or covert monitoring of human activity.

Additional information is available in the report: "Conduct Digital Surveillance Ethically and Legally: 2012 Update," which is available on Gartner's web site at http://www.gartner.com/resId=1965315

Mr Walls will be presenting on the threats and opportunities of monitoring users for security intelligence at the upcoming Gartner Security & Risk Management Summits 2012 in National Harbour, Maryland, Sydney, Australia, and London, UK.

About Gartner Security & Risk Management Summit
The Gartner Security & Risk Management Summit features four programmes focusing on Security, Risk Management and Compliance, Business Continuity Management and chief information security officer (CISO) roles to deliver detailed, role-specific content and networking. Each programme offers a full agenda of analyst sessions, keynotes, roundtable discussions, case studies, workshops and more.

For additional details about the Gartner Security & Risk Management Summit 2012 taking place 19-20 September in London, please visit www.gartner.com/eu/security. Members of the media can register by contacting laurence.goasduff@gartner.com.

Additional information from the event will be shared on Twitter at http://twitter.com/Gartner_inc and using #GartnerSEC.

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 the valuable partner to clients in 12,000 distinct organisations. Through the resources of Gartner Research, Gartner Executive Programs, Gartner Consulting and Gartner Events, Gartner works with every client to research, analyse and interpret the business of IT within the context of their individual role. Founded in 1979, Gartner is headquartered in Stamford, Connecticut, U.S.A., and has 5,000 associates, including 1,280 research analysts and consultants, and clients in 85 countries. For more information, visit www.gartner.com.

# # #