HealthManagement
Promoting Management and Leadership

IDC Forum: Staff Training Critical for IT Security

The ‘good guys’ are much more organised and targeted than the ‘bad guys’ which is contributing to the rise in data breaches around the globe, Paschalis Pissarides, of the Information Systems Audit and Control Association (ISACA) said at the IDC IT Management Forum in Nicosia. “This is war and we must use military tactics and strategy to win it,” he added

Pissarides said that the top reasons for poor IT security included a lack of cyber security awareness, centralised monitoring, poor information classification, a weak incident response plan and a lack of network segmentation.

Importantly, staff training on cyber security was widely overlooked in all sectors and company sizes.

This view was echoed by eight other speakers from Banking, Financial Services, Transportation, Utilities, Logistics, Telecommunications, Government and Public Administration and Manufacturing sectors.

“It takes an average of seven months to identify a breach and a further two months to address it,” Pissarides said. “All of the companies I deal with say there is a huge skills gap. There are too many IT security risks and too few professionals to deal with them.”

Amongst the measures to fight data breaches, the speakers suggested:

- Establishment of a Security and Risk management to reduce risk;
- Use of information classification systems;
- Implementing measures for data leakage prevention;
- Centralising of system log collection and correlation;
- Staff training for better security awareness.

“Over the next five years, 90% of companies' IT investments will involve Third Platform technologies. While organisations will still need servers, PCs, client- and PC-based applications, and miles of cables, these technologies will serve mainly as tools to facilitate the use of mobility, cloud, Big Data analytics, and social networks. Architectures, communication processes, and IT contracts will change. Organisations' awareness of their capabilities and potential will increase dramatically,” Andy Hicks of IDC said.
See Also: Lack of Resources Frustrates Healthcare IT Security

The impact on operations will be wide-reaching and data security incidents were bound to rise. Studies showed that from 2010 to 2015, cyber criminals used increasingly advanced technology to access data.

Also on the agenda was energy efficiency for data centres, monetising data, and IT ecosystems.

Hicks also spoke about the challenges of bridging the gap between the tech and business departments in a company. “In years to come as personnel become more tech savvy, leadership will be dispersed throughout an organisation because staff will have equal access to information and have common goals.

International Data Corporation (IDC) is a global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. More than 1000 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For more than 47 years, IDC has provided strategic insights to IT professionals, business executives, and the investment community to help them achieve their key business objectives.

Source: IDC IT Management Forum

Image Source:

Published on : Wed, 30 Mar 2016