The Institute of Internal Auditors Singapore

MAY 2017

Were you Prepared for The Ransomware Attack?

The world's biggest-ever computer ransom assault in the month of May has affected more than 190 countries. The indiscriminate attack, which began on Friday, struck banks, hospitals and government agencies, exploiting known vulnerabilities in old Microsoft computer operating systems. According to the cyberattack message, payment is demanded within three days or the price is doubled, and if none is received within seven days the locked files will be deleted.

Was your organisation prepared? What is your role as internal auditor with regards to cybersecurity? The IIA’s Global Technology Audit Guide (GTAG) in Sep 2016 is a useful guidance for internal auditors. In addition, “GTAG: Assessing Cybersecurity Risk” describes internal audit’s role in cybersecurity including the CAE’s role relating to assurance, governance, risk, and cyber threats and the assessment of risks and threats. “GTAG: Auditing IT Governance” also provides further guidance for IT governance.

Cybersecurity will continue to top the list of risks for internal auditors, audit committees, senior management and board of directors. Internal auditors play an important role as part of its overall assurance responsibilities, to determine if cybersecurity risks are addressed effectively. In reporting to the audit committee, CAE should keep cybersecurity on the agenda, discuss the level of cyber resilience preparedness with audit committees. Internal auditors should also take a multi-prong approach i.e. from auditing people and culture on cybersecurity awareness and discipline, to risk management systems, policies and procedures and incident management framework. It is important for internal auditors to also share their insights in these areas with management and the Board.

Tan Boon Yen, CIA, CRMA
President
The Institute of Internal Auditors Singapore