@ISACA
RELEVANT, TIMELY NEWS
Volume 11, 26 May 2010

10 Tips for IT Supply Chain Security and Risk Management

By John P. Pironti, CISA, CISM, CGEIT, ISSAP, ISSMP

1. If clients or partners ask you to fill out a questionnaire that includes sensitive information about how you secure their data, make sure you ask them for the same or allow them to view the information onsite only, at your premises. This ensures that your sensitive security information is cared for properly in its environment.
2. Always include a right-to-audit statement in your contracts with vendors and partners that allows you to perform security audits of their environments with limited or no notice.
3. When utilizing custom-code development services, make sure you have the source code reviewed by a reputable third party or use source-code scanning tools to ensure that bugs and security vulnerabilities are exposed and remediated prior to acceptance and implementation.
4. Ensure you have at least two vendors who can provide the same quality and quantity of IT services for critical IT functions that you outsource to ensure redundancy in the case of a failure of any one vendor.
5. Develop and maintain business process maps, which detail all IT supply chain dependencies and requirements for key business processes.
6. Conduct random security audits of vendor's facilities and capabilities at least once per year.
7. Categorize your vendors based on the level of access to sensitive materials they work with or access, and apply controls and oversight based on this categorization.
8. Meet with vendors in your IT supply chain at least once per year to brief them on your policies, requirements and expectations of how they will secure your information.
9. Develop an information security intelligence sharing network among the vendors

in your IT supply chain to share insights and information on a regular basis.

10. Establish and monitor key performance indicators and thresholds for these indicators for key IT business processes that utilize third-party capabilities to provide intelligence about the health and safety of your IT supply chain.

John P. Pironti, CISA, CISM, CGEIT, ISSAP, ISSMP, is the president of IP Architects LLC.