New NIST publication provides guidance for computer security risk assessments

19 September 2012

The National Institute of Standards and Technology has released a final version of its risk assessment guidelines that can provide senior leaders and executives with the information they need to understand and make decisions about their organization's current information security risks and information technology infrastructures.

"Risk assessments are an important tool for managers," explains Ron Ross, NIST fellow and one of the authors of Guide for Conducting Risk Assessments. "With the increasing breadth and depth of cyber attacks on federal information systems and the U.S. critical infrastructure, risk assessments provide important information to guide and inform the selection of appropriate defensive measures so organizations can respond effectively to cyber-related risks."

Information technology risks include risk to the organization's operations (including, for example, missions and reputation), its critical assets such as data and physical property, and individuals who are part of or served by the organization. In some cases, these risks extend to the nation as a whole. Risk assessments are part of an organization's total risk management process.

In March 2011, NIST released Managing Information Security Risk: Organization, Missions and Information System View (NIST Special Publication 800-39), which describes the process for managing information security risk for federal agencies and contractors. That process includes framing risk, assessing risk, responding to risk and monitoring risk over time.

The new publication, *Guide for Conducting Risk Assessments*, focuses exclusively on risk assessment—the second step in the information security risk management process. The guidance covers the four elements of a classic risk assessment: threats, vulnerabilities, impact to missions and business operations, and the likelihood of threat exploitation of vulnerabilities in information systems and their physical environment to cause harm or adverse consequences.

"As the size and complexity of our collective IT infrastructure grows, we cannot protect everything we own or manage to the highest degree," says Ross. "Risk assessments show us where we are most at risk. It provides a way to decide where managers should focus their attention."

The risk assessment guidance is designed to meet the needs of a variety of organizations, large and small, including financial institutions, health care providers, software developers, manufacturing companies, military planners and operators, and law enforcement groups.

The Guide for Conducting Risk Assessments (SP 800-30, Revision 1) completes the original series of five key computer security documents envisioned by the Joint Task Force—a partnership of NIST, the Department of Defense, the Office of the Director of National Intelligence and the Committee on National Security Systems—to create a unified information security framework for the federal government. SP 800-39 is also in this series.

The guide is available at www.nist.gov/manuscript-public … ch.cfm?pub_id=912091 .

Provided by National Institute of Standards and Technology