New publication fundamentally changes federal information security risk management

March 2 2011, By Evelyn Brown

The National Institute of Standards and Technology (NIST) has published the final version of a special publication that can help organizations to more effectively integrate information security risk planning into their mission-critical functions and overall goals.

Managing Information Security Risk: Organization, Mission, and Information System View (NIST Special Publication 800-39) provides the groundwork for a three-tiered, risk-management approach that "fundamentally changes how we manage information security risk at the federal level," says Ron Ross, NIST Fellow and one of the principal authors of the publication.

For decades, organizations have managed risk at the information system level that resulted in a very narrow perspective that constrained risk-based decisions by senior management, Ross explains. SP 800-39 calls for a holistic approach in which senior leaders determine what needs to be protected based on the organization's core missions and business functions. For example, managers of a power plant tied to the distribution grid need to ensure that its computer security keeps hackers from interfering with the plant's power generation or getting into the power grid to wreak greater havoc.

The publication is the fourth in the series of risk management and information security guidelines being developed by the Joint Task Force

Transformation Initiative, a joint partnership among the Department of Defense, Intelligence Community, NIST and the Committee on National Security Systems.

The multi-tiered risk management approach described in SP 800-39 progresses from organization to missions to information systems. The goal is to ensure that strategic considerations drive investment and operational decisions with regard to managing risk to organizational operations (including mission, function, image and reputation), organizational assets, individuals, other organizations (collaborating or partnering with federal agencies and contractors) and the nation.

This type of risk-based, decision making is critical as organizations address advanced persistent threats of sophisticated cyber attacks that have the potential to degrade or debilitate information systems supporting the federal government's critical applications and operations.

"SP 800-39 is about building more secure information systems which will ultimately allow senior leaders and executives to better understand the mission and business risk brought into their enterprises by the ever-increasing use of, and dependence on, information technology and network connectivity," Ross says.

More information: SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, has been developed in support of the Federal Information Security Management Act (FISMA). It can be downloaded from csrc.nist.gov/publications/nis … 9/SP800-39-final.pdf

Provided by National Institute of Standards and Technology

Citation: New publication fundamentally changes federal information security risk management (2011, March 2) retrieved 23 April 2024 from https://phys.org/news/2011-03-fundamentally-federal.html