

Fact Sheet

Information Technology Sector

Products and Services, Incident Management, and Internet Routing

Risk Management Strategies

PURPOSE: Public and private owners and operators completed the first-ever functions-based Information Technology (IT) Sector Baseline Risk Assessment in August 2009. This assessment describes risks from manmade deliberate, manmade unintentional, and natural threats to producers and providers of IT hardware, software, and services using threat, vulnerability, and consequence frameworks. The IT Sector Risk Assessment (ITSRA) resulted in an IT Sector Risk Profile that identifies national-level risks of concern for the IT Sector. Public and private sector partners collaboratively developed the assessment, which reflects the expertise of participating subject matter experts (SME). Using the risks identified in the ITSRA, IT Sector partners systematically addressed the risks of concern for each of the IT Sector's critical functions by engaging in risk management analyses. Where necessary, they also defined and proposed mitigation strategies to reduce national level risks.

The Information Technology Sector Risk Management (ITSRM) Strategies for the *Produce and Provide IT Products and Services* function; *Provide Incident Management Capabilities* function; and *Provide Internet routing, access, and connection services* function identify response and mitigation strategies designed to manage risks of concern that were identified in the 2009 ITSRA. The strategies inform industry and government organizations of the IT Sector's risk management priorities and activities and explain how their implementation improves the security of the IT Sector.

APPROACH: Using the risks identified in the ITSRA, IT Sector partners developed ITSRM strategies. These strategies identify appropriate risk responses for the risks of concern to each IT Sector critical function, and where necessary, also define and propose mitigation strategies to reduce national level risks for four of the IT Sector critical functions:¹

- Providing domain name resolution services;²
- Producing and providing IT products and services;
- Providing incident management capabilities; and,
- Providing Internet routing, access and connection services.

Identifying risk responses and prioritizing the mitigations for identified IT Sector risks helps ensure that resources are applied where they can most effectively respond to the threats, vulnerabilities, and consequences facing the critical IT Sector functions. Also, following the baseline ITSRA, sector partners are performing in-depth

Critical IT Sector Functions

- Producing and providing IT products and services
- Providing incident management capabilities
- Providing domain name resolution services
- Providing identity management and associated trust services
- Providing Internet-based content, information and communications services
- Providing Internet routing, access and connection services

¹ The risk mitigation strategies for the *Provide domain name resolution services* and the *Provide Internet routing, access and connection services* address the risks of concern for the *Provide Internet-based content, information and communications services* critical function. As such, IT Sector partners will not be developing a separate Internet Content risk mitigation strategy.

² The risk mitigation strategy for the *Provide domain name resolution services* function was released on June 17, 2011.

risk assessments on the *Providing identity management and associated trust services* critical function and a risk assessment to examine IT Sector dependencies on the Energy and Communications Sectors.

FINDINGS:

Description	ITSRA Risks of Concern	Risk Mitigation Strategies
<p><i>Produce and Provide IT Products and Services:</i> The IT Sector conducts operations and services that provide for the design, development, distribution, and support of IT products—such as hardware and software—and operational support services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.</p>	<ul style="list-style-type: none"> • Production or distribution of untrustworthy critical product/service through a successful manmade deliberate attack on a supply chain vulnerability; • Failure or disruption in distribution of a critical service or product; and • Failure or disruption in production of a critical service or product. 	<p>The IT Sector Products and Services Risk Management Strategy includes a portfolio of risk mitigation activities that mitigate key risks, such as:</p> <ul style="list-style-type: none"> • Untrustworthy Product or Service – Enhance supply chain delivery mechanisms to minimize counterfeiting and tampering; • Distribution Failure or Disruption – Develop, establish, and/or adopt IT Sector standards and/or best practices; • Production Failure or Disruption – Increase awareness among the acquirers and suppliers of IT products and services of need to manage business risk.
<p><i>Provide Incident Management Capabilities:</i> The IT Sector develops, provides, and operates incident management capabilities for itself and other sectors that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.</p>	<ul style="list-style-type: none"> • Impact to detection capabilities due to a lack or unavailability of risk-related data, which is caused by a natural hazard; • Impact to detection resulting from a manmade deliberate falsification of incident report data; and • Impact to response capabilities due to a manmade deliberate exploitation of capabilities that prevent or render a type of attack. 	<p>The IT Sector Incident Management Strategy includes a portfolio of risk mitigation activities that mitigate key risks, such as:</p> <ul style="list-style-type: none"> • Lack of Data – Improve redundancy and distribution of resources and data; • Falsified Reports – Educate the workforce to recognize falsified information and validate sources (training and awareness); and • Inability to Prevent or Render – Invest in or develop alternative data delivery capabilities to use when primaries are unavailable.
<p><i>Provide Internet Routing, Access, and Connection Services:</i> The IT Sector provides and supports Internet backbone infrastructures, points of presence, peering points, local access services and capabilities that are essential or critical to the assurance of national and economic security and public health, safety and confidence.</p>	<ul style="list-style-type: none"> • A partial or complete loss of routing capabilities, either locally, regionally, or across large parts of the world, caused by deliberate or unintentional actions; • Natural disasters or manmade incidents that could impair the operation of concentrated routing facilities; and • Ineffective or impaired responses to restoring routing operations after an outage or an incident 	<p>The IT Sector Internet Routing Risk Management Strategy includes a portfolio of risk mitigation activities that mitigate key risks, such as:</p> <ul style="list-style-type: none"> • Partial or complete loss of routing capabilities – Formulate and apply appropriate local routing policy; • Natural disasters or manmade incidents that could impair the operation of concentrated routing facilities - Take extensive steps to secure facilities from physical attacks and natural disasters; and • Ineffective or impaired responses to restoring routing operations after an outage or an incident – Develop a comprehensive incident management and incident recovery plan.



BACKGROUND: Homeland Security Presidential Directive-7 established a national policy for federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect those resources from attack. The DHS National Cyber Security Division (NCSA) serves as the Sector Specific Agency (SSA) for the IT sector and as a focal point for the security of cyberspace and facilitates interactions and collaborations between and among federal departments and agencies; state, local and tribal governments; the private sector; academia; and international organizations. The DHS National Infrastructure Protection Plan (NIPP) provides the unifying structure to integrate the existing and future critical infrastructure protection (CIP) efforts into a single national program.

The NIPP describes a sector partnership model that encourages the public and private sectors to collaborate on their respective infrastructure protection activities. Both the IT Government Coordinating Council (GCC), composed of government representatives, and the IT Sector Coordinating Council (SCC), composed of IT Sector industry members, serve as the primary bodies for the communication of public and private perspectives and the coordination of collaborative strategies, policies, and security efforts that advance CIKR protection for the Sector.