

Information Technology Sector



Risk Management Strategy for the *Produce and Provide IT Products and Services Critical Function*

July 2011

Contents

Executive Summary	1
1 Information Technology Sector Risk Management Overview.....	4
2 Risk Overview – <i>Produce and Provide IT Products and Services</i> Critical Function.....	5
3 Produce and Provide IT Products and Services Risk Management Strategy	9
3.1 Risk of Concern – Untrustworthy Product or Service (Manmade Deliberate)	11
3.1.1 Risk Overview.....	11
3.1.2 Risk Response.....	12
3.2 Other Risks of Concern – Failure or Disruption of Production or Distribution (Manmade Deliberate, Manmade Unintentional, Natural)	18
3.2.1 Risk Overview.....	18
3.2.2 Risk Response.....	20

Figures

Figure 1: IT Sector Products and Services Value Chain	6
Figure 2: Produce and Provide IT Products and Services Attack Tree (Summary)	8
Figure 3: Produce and Provide IT Products and Services Relative Risk Table.....	8
Figure 4: Untrustworthy Product or Service Attack Tree	12
Figure 5: Effectiveness of Proposed Mitigation Strategy to Untrustworthy Product or Service	15
Figure 6: Distribution Failure Attack Tree	19
Figure 7: Production Failure or Disruption Attack Tree.....	19

Tables

Table 1. Risk and Mitigation Overview.....	2
Table 2: IT Sector’s High Consequence Risk for Produce and Provide IT Products and Services.....	5
Table 3: Untrustworthy Product or Service Risk and Mitigation Overview	10
Table 4: Feasibility of Proposed Mitigation Strategy to Untrustworthy Product or Service	16
Table 5: Risk and Mitigation Overview.....	20

Executive Summary

Public and private IT Sector owners and operators completed the first ever functions-based risk assessment in August 2009. The IT Sector Baseline Risk Assessment (ITSRA) assesses risks from manmade deliberate, manmade unintentional and natural threats using threat, vulnerability, and consequence frameworks within the Sector's risk assessment methodology. The ITSRA resulted in a comprehensive baseline 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 and collective consensus of participating subject-matter experts (SME).

Sector partners are systematically addressing the risks of concern for each critical function by engaging in risk management analyses wherein SMEs assess the merits and drawbacks of taking one of four approaches to risk mitigation:

- Avoid the risk;
- Accept the risk and its potential consequences;
- Transfer the risk to another sector or entity; or
- Mitigate the risk by preventative or proscriptive action.

Where mitigation is the preferred risk response, IT Sector partners identify appropriate Risk Mitigation Activities (RMA) to reduce national-level risks across each critical function based on SME input. The identified risk responses and the prioritization of the mitigations for identified IT Sector risks will inform resource allocation to most effectively respond to the threats, vulnerabilities, and/or consequences facing the critical IT Sector functions. IT Sector partners analyzed the ITSRA risks of concern to the *Produce and Provide IT Products and Services* critical function and developed mitigation responses to three risks of concern. The risks, associated RMAs, and resulting likelihood and consequence ratings appear in Table 1.

Critical IT Sector Functions

- Provide IT products and services*
- Provide incident management capabilities*
- Provide domain name resolution services*
- Provide identity management and associated trust support services*
- Provide Internet-based content, information, and communications services*
- Provide Internet routing, access, and connection services*

Table 1. Risk and Mitigation Overview

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings ¹
Untrustworthy Product or Service	Low likelihood; high consequence	<ul style="list-style-type: none"> □ Develop, establish, and/or adopt IT Sector standards and/or best practices □ Use established standards and best practices to establish acquisition practices to articulate specific requirements and monitoring practices for product components and raw materials development, delivery, and integration 	Low Likelihood; high consequence ²
Distribution Failure or Disruption	Low likelihood; low consequence	<ul style="list-style-type: none"> □ Enhance supply chain delivery mechanisms to minimize counterfeiting and tampering, such as implementing point verification along the supply chain (e.g., radio-frequency identification (RFID) or holograms) and using anti-counterfeiting techniques to ensure authenticity of system and network components 	Low likelihood; low consequence
Production Failure or Disruption	Low likelihood; medium consequence	<ul style="list-style-type: none"> □ Increase awareness among the acquirers and suppliers of IT products and services of need to manage business risk, including for natural disasters, supply chain intrusion/insertion, and anti-counterfeiting 	Low likelihood; medium consequence

The final RMA strategies will inform the 2011 IT Sector Annual Report (SAR), which is the primary way through which Critical Infrastructure and Key Resources (CIKR)-sector R&D efforts and priorities are captured. IT Sector cybersecurity R&D requirements will be identified in the SAR and serve as inputs into the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) processes for identifying and addressing R&D needs. The report will also influence cross-sector cybersecurity R&D needs and requirements and recommendations made with regard to those areas where the U.S. Government should make focused investments.

Additionally, the final RMA strategies will be delivered to the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), which provides a forum for Federal Departments/Agencies to exchange program-level R&D information. The IT Sector maintains an active relationship with the CSIA

1 Assumes complete implementation of the items noted in the Risk Mitigation Activities column

2 While the overall resulting risk and consequence ratings remain the same, implementing the risk mitigation activities does lower the likelihood of a threat exploiting the vulnerability; the consequence remains unchanged. For more details, refer to 3.1.2.

IWG and will use the results and recommendations contained in this report to coordinate to highlight key points of concern where both groups can work together to develop targeted R&D efforts to address issues raised by the final RMA strategies. Further, a number of key public forums will discuss issues that will shape and influence issues surrounding IT products and services and associated supply chain risks both now and in the future and will likely affect the issues raised by the recommendations made in this strategy.

The IT Sector Plans, Reports, and Risk Management Working Group is currently developing strategies for the remaining functions as outlined in the ITSRA. This report coupled with similar efforts across the other critical functions will provide a foundation for comprehensive IT Sector national-level risk reduction.

The remainder of this document:

- ❑ Provides an overview of the IT Sector's risk management approach;
- ❑ Discusses the risks of concern from the ITSRA;
- ❑ Details the SME-developed risk response strategies and risk mitigation activities; and
- ❑ Examines the effectiveness and feasibility of the risk mitigation activities.

1 Information Technology Sector Risk Management Overview

The National Infrastructure Protection Plan (NIPP), initially developed and published in 2006 and revised in 2009, specifically assigned the Department of Homeland Security (DHS) the mission of establishing uniform policies, approaches, guidelines, and methodologies for integrating infrastructure protection and risk management activities within and across CIKR sectors, along with developing metrics and criteria for related programs and activities. Using the NIPP and the IT Sector-Specific Plan (SSP), the IT Sector has been able to provide a consistent, unifying structure for integrating existing and future critical infrastructure protection and resilience efforts.

Partnership and collaboration between the IT Sector Coordinating Council (SCC) and the Government Coordinating Council (GCC) enables the Sector to leverage its unique capabilities to address the complex challenges of CIKR protection, providing both products and services that support the efficient operation of today's global information-based society.

The IT Sector uses a top-down and functions-based approach to assess and manage risks to its six critical functions to promote the assurance and resiliency of the IT infrastructure and to protect against cascading consequences based on the Sector's interconnectedness and the critical functions' interdependencies. IT SCC and GCC partners determined that this top-down and functions-based approach would be effective for the highly distributed infrastructure that enables entities to produce and provide IT hardware, software, and services. The top-down approach enables public and private IT Sector partners to prioritize additional mitigations and protective measures to risks of national concern.

The IT Sector Baseline Risk Assessment (ITSRA), released in 2009, serves as the foundation for the Sector's national-level risk management activities.³ Public and private sector partners collaborated to conduct the assessment, which reflects the expertise and collective consensus of participating subject matter experts (SMEs). The ITSRA methodology assesses risks from manmade deliberate, manmade unintentional and natural threats that could affect the ability of the Sector's critical functions and sub-functions to support the economy and national security. The methodology leverages existing risk-related definitions, frameworks, and taxonomies from a variety of sources, including public and private IT Sector partners, standards development organizations, and policy guidance entities. By leveraging these frameworks, the IT Sector's methodology reflects current knowledge about risk and adapts them in a way that enables a functions-based risk assessment.

The following table highlights the IT Sector's high consequence risk within the *Produce and Provide IT Products and Services* function as it appeared in the ITSRA. This high-consequence risk was identified by SMEs in a collaborative and iterative process that consisted of attack tree development, risk evaluation, and final analysis. The risk captured in the *Risk of Concern* column of the table highlights the highest consequence risk that could impact the confidentiality, integrity, or availability of the critical function. The *Mitigations* column is a summary of the mitigations identified in the ITSRA and were later validated through follow-on IT Sector Risk Management (ITSRM) sessions to address the highlighted risks.

³ The ITSRA is available at the following URL:
http://www.it-scc.org/documents/itscc/IT_Sector_Risk_Assessment_Report_Final.pdf

Table 2: IT Sector’s High Consequence Risk for Produce and Provide IT Products and Services

Critical IT Sector Function	Risk of Concern	Mitigations (Existing, Being Enhanced, or Potential Future)
Produce and Provide IT Products and Services	<ul style="list-style-type: none"> <input type="checkbox"/> Production or distribution of untrustworthy critical product/service through a successful manmade deliberate attack on a supply chain vulnerability (<i>Consequence: High; Likelihood: Low</i>) 	<ul style="list-style-type: none"> <input type="checkbox"/> Supply chain resiliency through redundancy and process controls - <i>Existing Mitigation</i> <input type="checkbox"/> Sourcing strategies (i.e., careful monitoring of the availability and quality of critical raw materials) - <i>Existing Mitigation</i> <input type="checkbox"/> Product recall or update (such as a software patch) informed by situational awareness and timely response to compromised production - <i>Existing Mitigation</i>

For the risks of concern, IT Sector partners engaged in risk management analyses wherein SMEs assessed the merits and drawbacks of taking one of four approaches to risk management. The four approaches are:

- Avoid the risk;
- Accept the risk and its potential consequences;
- Transfer the risk to another sector or entity; or,
- Mitigate the risk by preventative or proscriptive action.

Where mitigation emerged as the preferred risk response, IT Sector partners identified appropriate RMAs to reduce national-level risks across each critical function based on SME input. The identified risk responses and the prioritization of the mitigations for identified IT Sector risks help to inform resource allocation to most effectively respond to the threats, vulnerabilities, and/or consequences facing the critical IT Sector functions. The remainder of this document discusses the risk responses and associated RMAs for the IT Sector *Produce and Provide IT Products and Services* critical function.

2 Risk Overview – Produce and Provide IT Products and Services Critical Function

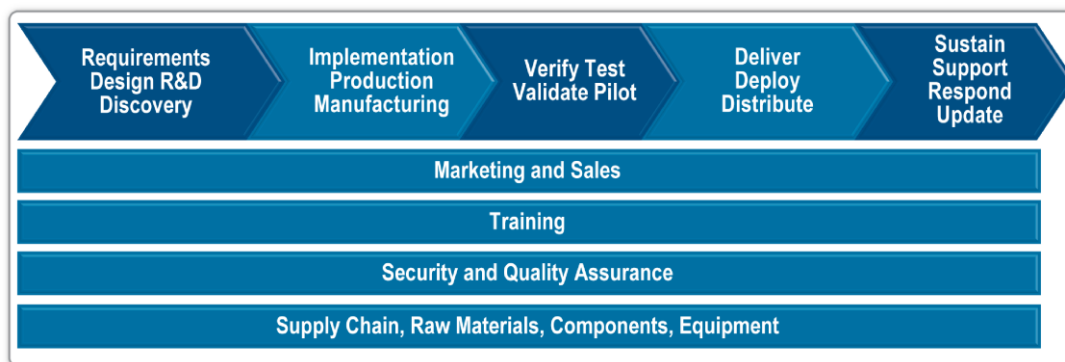
Produce and Provide Domain Name Resolution Services Function Summary	
Situation	Hardware and software products are designed, developed, and distributed throughout the world, and many of the manufacturing inputs required—whether physical materials or intellectual capital—are globally sourced.
Concern	Attacks against and exploitation of IT products can occur anywhere in the world at any time. Thus, producers and providers of hardware and software must remain diligent and aggressive in addressing risks to their global operations that support this function.
Impact	While incidents impacting the availability of the supply chain to support the production of IT products and services are frequently mitigated to acceptable levels of risk, there are relatively greater risks associated with the integrity and confidentiality impacts to the function.

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. These nationally significant hardware and software products and services maintain or constitute networks and associated services. The specific sub-functions related to the *Produce and Provide IT Products and Services* critical function are:

- Produce and provide networking elements;
- Produce and provide security and policy compliance elements;
- Produce and provide operating system services software;
- Produce and provide business operations, database, and business intelligence software and services;
- Produce and provide managed network/data center elements;
- Produce and provide semiconductors;
- Produce and provide storage hardware, software, and services;
- Provide lifecycle product and service integrity, certification, and other assurance functions and mechanisms;
- Develop DNS software;⁴
- Develop and provide secure appliances that support DNS;⁵ and
- Produce and provide control systems products, Supervisory Control and Data Acquisition (SCADA), and other automation systems.

Providing hardware and software to consumers relies on the IT Sector's ability to produce and distribute trustworthy products. The key elements of the function's operations include the availability of raw materials; effective processes that support both manufacturing and quality assurance; and a resilient yet efficient supply chain that supports the development, manufacturing, and distribution aspects of the value chain.

Figure 1: IT Sector Products and Services Value Chain



Hardware and software products are designed, developed, and distributed throughout the world, and many of the manufacturing inputs required—whether physical materials or knowledge—are acquired on a global scale. This fosters a competitive market that provides consumers with high quality and cost-effective products. The global nature of the function also results in the risk of attacks against, and exploits of, IT products anywhere in the world at any time. Thus, producers and providers of hardware

⁴ For an assessment of the risk to the Domain Name System's operations, please see the section related to the *Provide Domain Name Resolution Services* function.

⁵ For an assessment of the risk to the Domain Name System's operations, please see the section related to the *Provide Domain Name Resolution Services* function.

and software must remain diligent and active in addressing risks to their global operations that support this function.

In addition, IT products are often comprised of elements that are themselves IT products with their own individual supply chains. As a result, the IT Sector has similar but different practices it must apply to the acquisition of raw materials and components. These concerns make securing the IT supply chain even more complex.

Despite the broad scope and diversity across the *Produce and Provide IT Products and Services* function and sub-functions, risks to the availability of producing and providing IT products and services are generally managed to acceptable levels by IT Sector vendors and suppliers themselves. Producers carefully monitor the availability of all critical materials and components and identify multiple sources to mitigate dependency risks. This “many-to-many” relationship creates significant capacity and redundancy margins that can accommodate even catastrophic shortages. Also, the producers and providers of the function have response capabilities that address the frequently predictable nature of most attacks, and these response capabilities are rehearsed and well-planned. If the function is severely damaged, market forces usually enable producers and providers to utilize new resources before shortages cause national- or sector-level impacts. Producers and providers also maintain sufficient sourcing strategies and stockpiles to outlast most raw materials shortages until replacements are found.

In addition, the consumers of the products and services are also part of managing risk in the supply chain. For example, it is incumbent upon consumers to verify the authenticity of the products and services they purchase and to only acquire products and services from reputable sources. Organizations must also employ careful planning of sustainment practices for systems and devices, including how to purchase necessary replacement parts in a secure manner, especially because parts may no longer be widely available.

IT Sector SMEs developed attack trees during the ITSRA to evaluate the Consequences [C], Vulnerabilities [V], and Threats [T] associated with the critical functions. The attack trees illustrate undesired consequences, vulnerabilities that can lead to those undesired consequences, and the threats that can exploit the vulnerabilities. The attack trees used to analyze IT Sector risks in the ITSRA and to scope risk response strategies are depicted in the Risks of Concern section within this document.

As detailed in Figure 2, SMEs assessed risk to the function using an attack tree that focused on three undesired consequences that could cause adverse effects on supply chains at the national level. Because of the wide range of vulnerabilities within the Produce and Provide IT Products and Services function, SMEs examined manmade deliberate, manmade unintentional and natural threats to categorize possible methods by which a consequence could occur.

Figure 2: Produce and Provide IT Products and Services Attack Tree (Summary)

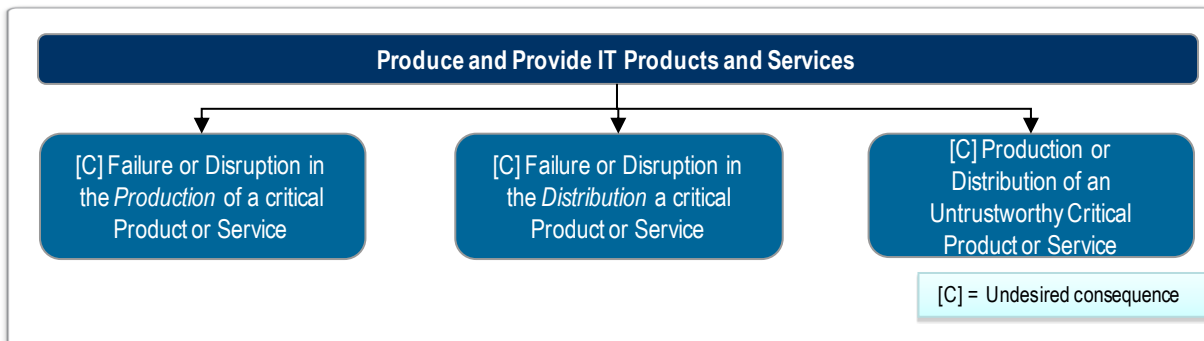


Figure 3 shows the risk profile for the *Produce and Provide IT Products and Services* critical function that was developed as part of the 2009 ITSRA. This matrix maps the likelihood of each threat exploiting a products and services vulnerability (Y-axis) against the relative consequences as a result of that threat exploiting vulnerability (X-axis). The highlighted risk is the only high-consequence risk.

Figure 3: Produce and Provide IT Products and Services Relative Risk Table

Likelihood of threat exploiting vulnerability	High				
	Medium		<ul style="list-style-type: none"> Supply chain vulnerability: Failure or disruption in the production of a critical product/service (Manmade Unintentional) 	<p>Supply chain vulnerability: Production or distribution of an untrustworthy critical product/service (Manmade Deliberate)</p>	
	Low	<ul style="list-style-type: none"> Supply chain vulnerability: Failure or disruption in the distribution of a critical product/service (Manmade Deliberate) Supply chain vulnerability: Failure or disruption in the distribution of a critical product/service (Manmade Unintentional) 	<ul style="list-style-type: none"> Supply chain vulnerability: Failure or disruption in the production of a critical product/service (Manmade Deliberate) 	<ul style="list-style-type: none"> Supply chain vulnerability: Production or distribution of an untrustworthy critical product/service (Manmade Deliberate) 	
	Negligible				
		Negligible	Low	Medium	High
		Relative consequences resulting from successful exploitation by threat			
		Bold Text	<i>Risk of Concern</i>		<i>Expanded view for Risk of Concern</i>

3 Produce and Provide IT Products and Services Risk Management Strategy

This section describes the risk management strategies that were proposed for the function's high-consequence risk. That risk, as identified in the ITSRA, is:

- ❑ Untrustworthy Product or Service (Manmade, Deliberate)

IT Sector partners resolved to pursue *Mitigate the risk by preventative or proscriptive action* as the selected response. However, the IT Sector partners noted that many of the risks to the IT supply chain are difficult to address with approaches that target a specific vulnerability. IT Sector supply chains are numerous, diverse, distributed and global, containing a wide variety of vendors and suppliers. As a result, risks posed to each supply chain vary broadly depending on the specific threats and vulnerabilities of that supply chain and on the security practices of each vendor or supplier in a particular supply chain lifecycle. For example, threats posed to hardware supply chains are different from threats posed to software supply chains. Software supply chains are subject to "logical" disruptions, such as the insertion of malicious code, while hardware supply chains face physical disruptions such as the insertion of counterfeit products into the supply or the disruption of distribution processes. Due to the dynamic supply chain risk landscape and need for very specific mitigations and countermeasures, risks are often addressed at the organizational level, and mitigation strategies include actions and insights from individual vendors and suppliers.

With that caveat in mind, the IT Sector partners noted that there are still some national- and sector-level approaches that can be adopted in order to mitigate the risks to this function.

Table 3 illustrates the risk mitigation activities associated with the risk of producing or distributing an untrustworthy product/service.

Table 3: Untrustworthy Product or Service Risk and Mitigation Overview

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings ⁶
<p>Untrustworthy Product or Service</p>	<p>Low likelihood; high consequence</p>	<ul style="list-style-type: none"> ❑ Develop, establish, and/or adopt IT Sector standards and/or best practices ❑ Use established standards and best practices to establish acquisition practices to articulate specific requirements and monitoring practices for product components and raw materials development, delivery, and integration ❑ Enhance supply chain delivery mechanisms to minimize counterfeiting and tampering, such as implementing point verification along the supply chain (e.g., radio-frequency identification (RFID) or holograms) and using anti-counterfeiting techniques to ensure authenticity of system and network components ❑ Increase awareness among the acquirers and suppliers of IT products and services of need to manage business risk, including for natural disasters, supply chain intrusion/insertion, and anti-counterfeiting 	<p>Low Likelihood; high consequence⁷</p>

Given the integrated nature of IT supply chains, IT Sector partners observed that the recommended risk mitigation activities for this risk would also apply to the other ITSRA-identified risks of concern; in particular, risks to either the production or distribution of a critical product/service (see Section 3.2). As such, IT Sector partners analyzed the risk mitigations with a primary focus on untrustworthy products or services with the implicit understanding that the risk mitigations would also apply to disruption in the production of products and services and disruption in the distribution of products and services.

⁶ Assumes complete implementation of the items noted in the Risk Mitigation Activities column

⁷ While the overall resulting risk and consequence ratings remain the same, implementing the risk mitigation activities does lower the likelihood of a threat exploiting the vulnerability; the consequence remains unchanged. For more details, refer to 3.1.2.

3.1 Risk of Concern – Untrustworthy Product or Service (Manmade Deliberate)

3.1.1 Risk Overview

The production or distribution of an untrustworthy product or service is serious risk to the IT Sector supply chain and remains the risk with the highest potential consequence. As noted in the ITSRA, threat actors include corporate spies, corrupt government officials, cyber vandals, disgruntled employees, foreign government agents or spies, nation-states, radical activists, and criminals. These threat actors can be motivated by a variety of concerns, such as financial gain, intelligence gathering (state-sponsored or corporate espionage), the desire to project power through capability demonstrations, or the desire to mislead consumers. The successful production or distribution of an untrustworthy product is likely to occur covertly and likely to be conducted by actors who are sophisticated, well-organized, and probably associated with larger entities such as nation-states or crime syndicates. Untrustworthy products or services may be physical, such as hardware embedded with a covert tracking or reporting device, or logical, such as untrustworthy software.

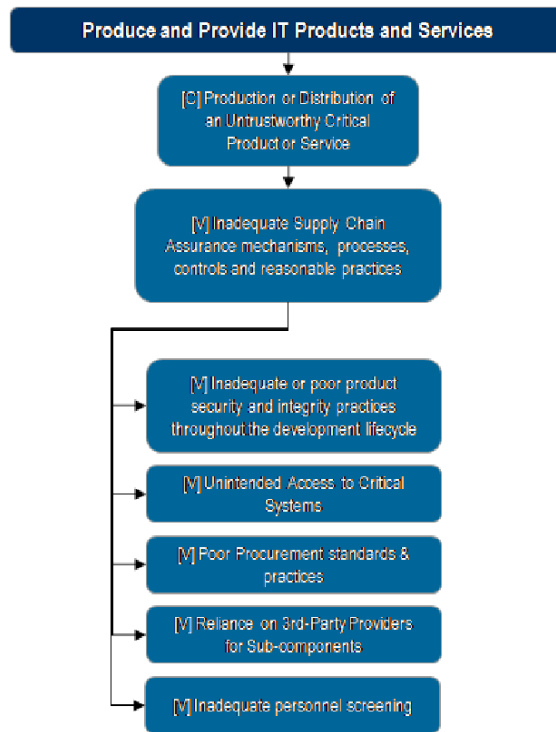
In recent years there have been several high-profile examples of this risk. For example, U.S. and Canadian law enforcement agencies seized more than \$78 million of counterfeit Cisco Systems networking equipment in 2008, including routers, switches, and network cards in an investigation of Chinese imports.⁸ Later that year, it was revealed that the FBI's Cyber Division was investigating the sale of such counterfeit equipment to the U.S. Department of Defense, Federal Aviation Administration, and the FBI.⁹

Risk assessment SMEs created the attack tree shown below in Figure 4 to identify vulnerabilities in IT supply chains that, if exploited, would result in the consequence of an untrustworthy product being produced or distributed. The attack tree provides the scope of the IT Sector's risk response strategy to this risk.

⁸ "Counterfeit gear seized by U.S., Canadian agencies." February 29, 2008. <http://www.infoworld.com/d/security-central/counterfeit-cisco-gear-seized-us-canadian-agencies-409>

⁹ "FBI worried DoD sold counterfeit Cisco gear." May 12, 2008. <http://www.infoworld.com/d/security-central/fbi-worried-dod-sold-counterfeit-cisco-gear-266>

Figure 4: Untrustworthy Product or Service Attack Tree



3.1.2 Risk Response

The ITSRA established that the national-level risk of a manmade, deliberate production or distribution of an untrustworthy product or service is *low likelihood* and *high consequence* (see Figure 3). IT Sector partners reached a consensus viewpoint that a combined mitigation strategy should be chosen as the appropriate risk response to this particular risk of concern, including:

- Develop, establish, and/or adopt IT Sector standards and/or best practices.
 - There are several ways in which the IT Sector can develop and integrate supply chain security best practices and standards. First, they can adopt the forthcoming International Organization for Standardization (ISO) on IT-specific supply chain issues, to be developed by the Joint Technical Committee (JTC) 1, Subcommittee (SC) 27. From this study, SC 27 has decided to restructure a standard currently under development, ISO/IEC 27036 (“Guidelines for security of outsourcing”), into a four-part standard titled “Information Security for Supplier Relationships.” This standard will include requirements that acquirers can use in contracts and information specific to supply chain risk management. It will cover all types of supplier relationships, including outsourcing, product and service acquisition, and cloud computing.
 - In addition, IT Sector members can develop additional standards or best practices or adopt best practice recommendations such as those recently developed by SAFECode in its report “Software Integrity Controls: An Assurance-Based Approach to Minimizing Risks in the Software Supply Chain.”¹⁰ IT Sector members can also participate in The Open Group, a vendor-neutral and technology-neutral consortium which works towards enabling access to integrated information within and between enterprises based on open standards and global interoperability.

¹⁰ http://www.safecode.org/publications/SAFECode_Software_Integrity_Controls0610.pdf

- Use established standards and best practices to establish acquisition practices to articulate specific requirements and monitoring practices for product components and raw materials development, delivery, and integration.
 - While there are no Sector-wide standards for IT supply chain security, there are numerous standards and best practices that can guide IT Sector partners. Notable examples include:
 - ISO/IEC 15288 – “System life cycle processes”
 - ISO/IEC 12207 – “Software life cycle processes”
 - ISO 28001 – “Best practices for implementing supply chain security, assessments and plans -- Requirements and guidance”
 - ISO 28002 – “Security management systems for the supply chain”
 - IEEE 1062 – “Recommended Practice for Software Acquisition”
 - ISO/IEC 15026 – “System and software integrity levels”
 - ISO 31000 – “Risk management -- Principles and guidelines”
 - ISO/IEC 27005 – “Information security risk management”
 - ISO/IEC 16085 – “Life cycle processes -- Risk management”
 - ISO/IEC 27001 – “Information security management systems – Requirements”
 - ISO/IEC 27002 – “Code of practice for information security management”
 - National Defense Industrial Association - Systems Assurance Guidebook
 - NIST IR 7622 – “Piloting Supply Chain Risk Management Practices for Federal Information Systems” (DRAFT)

- Enhance supply chain delivery mechanisms to minimize counterfeiting and tampering, such as implementing point verification along the supply chain (e.g., radio-frequency identification (RFID) or holograms) and using anti-counterfeiting techniques to ensure authenticity of system and network components.
 - Supply chain delivery mechanisms can be enhanced through either technological means or process improvements. Process improvements include actions such as using trusted, verified shippers or ensuring that suppliers have processes to detect differences in significant elements.¹¹ Point verification is an example of technology that can be used to improve supply chain security. Point verification controls provide supply chain partners with a means to verify the trustworthiness of products or components and to prevent counterfeit products from entering the supply chain. Two of the main types of these controls include RFID and holograms. RFID tags can provide IT Sector partners with the ability to verify that a particular component or product is trustworthy by tracking its progress through the supply chain lifecycle in order to ensure that it was only handled by trustworthy partners, thereby reducing the likelihood of compromise. Holograms are similar to RFID tags in that they can be used to track the lifecycle of a product or component, but are more secure because they embed the information in both RFID tags and holographic images, making the tags much harder and more expensive to counterfeit. While many of the IT Sector partners currently employ RFID technology, more extensive adoption of the technology or adoption of more secure RFID technology like holograms would further reduce supply chain vulnerabilities.

- Increase awareness among the acquirers and suppliers of IT products and services of need to manage business risk, including for natural disasters and supply chain intrusion/insertion.
 - One of the most effective and least costly ways to reduce these risks is to increase awareness across the IT Sector of business risks faced to the supply chain. Such efforts could include training and education, discussion forums, or the release of whitepapers. In addition, in order to improve all-around risk management practices, IT Sector partners need to be aware of the full spectrum of risks, which includes both manmade and natural threats.

¹¹ See Draft NISTIR 7622, Section 3.15 for a list of ways to improve processes. Though the document was written for Federal agencies, the methods described are applicable to all IT Sector partners.

These activities can be accomplished with the resources available to the IT Sector today and would not likely require additional research and development.

After formulating the combined risk mitigation strategy, IT Sector partners noted that the proposed measures would also benefit the rest of the functions of the IT Sector as the integrity of products used by those functions would improve; further, the mitigations would benefit all sectors which rely on the IT Sector to perform their own critical functions. Therefore, partners concluded that full nation-wide implementation of the proposed mitigation activities above would reduce the national-level risk beyond the improvements made directly in the *Produce and Provide IT Products and Services* function.

Although vulnerability is reduced slightly by implementing these measures, none of the proposed measures reduce the consequences if a vulnerability is exploited. However, the integrity of products and services to other IT Sector functions and the broader IT Sector increases the availability of the those critical operations that those functions provide, as well as increases the reliability of the sector to provide for its consumers.


Conversely, if these measures are not implemented, the likelihood of a threat exploiting supply chain vulnerabilities will increase. The ITSRA, the source of the likelihood and concerns addressed in this report, was first drafted in 2009. Since that time, threats have grown more sophisticated as adversaries improve their capabilities, as recently noted by U.S. Deputy Secretary of Defense William Lynn.¹² In addition, as the consequences have not changed during that time, the supply chain remains a high-profile target for attackers. As a result, if these and other security measures are not implemented, the likelihood of a threat actor successfully exploiting a vulnerability will only increase, especially because of increasing reliance on IT systems, software, and hardware by government, business, and individuals alike.

Figure 5 shows the original risk calculated by IT Sector partners and the resulting increase in risk if mitigations are not implemented.

¹² Lynn, William J. "Defending a New Domain: The Pentagon's Cyberstrategy." *Foreign Affairs*, September/October 2010.

Figure 5: Effectiveness of Proposed Mitigation Strategy to Untrustworthy Product or Service

Produce and Provide IT Products and Services Relative Risk Table

Likelihood of threat exploiting vulnerability	High				
	Medium		<ul style="list-style-type: none"> Supply chain vulnerability: Failure or disruption in the production of a critical product/service (Manmade Unintentional) 	<ul style="list-style-type: none"> Supply chain vulnerability: Production or distribution of an untrustworthy critical product/service (Manmade Deliberate) 	
	Low	<ul style="list-style-type: none"> Supply chain vulnerability: Failure or disruption in the distribution of a critical product/service (Manmade Deliberate) Supply chain vulnerability: Failure or disruption in the distribution of a critical product/service (Manmade Unintentional) 	<ul style="list-style-type: none"> Supply chain vulnerability: Failure or disruption in the production of a critical product/service (Manmade Deliberate) 		
	Negligible				
		Negligible	Low	Medium	High
		Relative consequences resulting from successful exploitation by threat			
		Bold Text	<i>Risk of Concern</i>		<i>Expanded view for Risk of Concern</i>

IT Sector partners were able to reach consensus on the feasibility of implementing the proposed risk management strategy (Table 3). Key feasibility considerations noted by IT Sector partners are noted as follows.

- ❑ Implementing point verification along the supply chain may cause legal requirements or issues.
- ❑ Standards are one of the IT Sector’s preferred methods to deal with risks. Standards allow the industry to address risks without government intervention. However, for several reasons there may still be pushback to the creation or adoption of new standards. International suppliers may have no profit motive to adopt such standards. In addition, the burden to comply with standards is placed on individual organizations, requiring them to expend their own time and resources to ensure compliance. This could also result be a cause of potential pushback. On the other hand, organizations may be more willing to accept standards if it will lead to a competitive advantage or the avoidance of a disadvantage. For example, if the adoption of standards leads to greater business for the competitors of a given company, that company is also likely to adopt those standards. Supplier countries may also be willing to adopt such standards since this adoption could differentiate entire countries as those whose companies are “more reliable” outsourcing service providers.

Table 4 shows the IT Sector partners' determinations of feasibility across several IT Sector SME-identified feasibility factors and the criteria by which those determinations were made.

Table 4: Feasibility of Proposed Mitigation Strategy to Untrustworthy Product or Service

Feasibility Factors	Feasibility	Description	Criteria	Explanation
Legal	Medium	Statutes, regulation	The existing legal framework needs adaptation to implement the proposed risk response.	Supply chains are global, and different countries have differing legal, regulatory, and export policies that are often not in harmony. While good practices have been developed, they are not implemented consistently across the board.
Organizational Compliance	High	Best practices, organizational charters, corporate values	The implementation of the proposed risk response aligns closely with the existing standards and best practices.	Standards are one of the sector's preferred methods for addressing risk, and organizations already adopt unmandated domestic and international best practices.
Political	Medium	Public confidence, privacy-related issues	There are limited political issues that may prohibit or inhibit the implementation of the risk response.	There are likely to be international pressures from overseas suppliers who will be resistive to change and have no profit motive to adopt such standards. However, this resistance may be partially offset by countries and/or suppliers willing to adopt standards as a means of differentiation.

Feasibility Factors	Feasibility	Description	Criteria	Explanation
Financial	Medium	Cost, budget limitations	Total average life-cycle costs for implementing the risk response can be only partially be covered via market forces and existing business models.	The burden will be placed on individual organizations to comply with standards and best practices, though this is not different from the adoption of any other standards. However, some organizations will take advantage of these standards to use compliance as a differentiator to sell products and services to those customers who really care.
Time	Medium	Reasonable schedule expectations	The implementation of the proposed risk response can be completed in a reasonable time frame (i.e., 13-24 months to full implementation).	It is unlikely that the development and adoption of standards would take less than 3 years.
Technology	High	Ease of implement existing technology or developing new technology	The risk response is relatively easy to implement or develop in the context of technological viability.	Technological implementation is not the issue, as the technology to implement these actions exists. Adoption of these mitigations is more likely to be driven by the political and market environments.
Market	Medium	Market conditions, competition	Market conditions are somewhat favorable to the implementation of the risk response	Competitors adopting standards will place pressure on those organizations who have not yet adopted.
Compatibility	Low	Confidentiality, Integrity, and Availability after implementation	Significant compatibility issues are associated with implementing the risk response.	It will remain difficult to verify multiple upstream sources along the supply chain, as supply chains have such a great number of partners that interact in various ways.

Feasibility Factors	Feasibility	Description	Criteria	Explanation
Cultural	High	The alignment of IT Sector culture and the risk response	The cultural environment of the IT sector facilitates the risk response well.	As long as regulation or mandates are not used, competitors adopting standards will place pressure on those organizations who have not yet adopted.

3.2 Other Risks of Concern – Failure or Disruption of Production or Distribution (Manmade Deliberate, Manmade Unintentional, Natural)

3.2.1 Risk Overview

The ITSRA identified several other risks posed to the IT supply chain. Namely, these risks are as follows:

- ❑ Failure or Disruption in *Distribution* of a Critical Service or Product (Manmade Deliberate, Manmade Unintentional)
- ❑ Failure or Disruption in *Production* of a Critical Service or Product (Manmade Deliberate, Manmade Unintentional)

IT Sector partners noted that both of these risks can be caused by a variety of threats and threat actors. *Manmade deliberate* threats are similar to the threat actors described previously in Section 3.1.1. *Manmade unintentional* (or accidental) threats include employees throughout the distribution, manufacturing, update, and sustaining aspects of the product lifecycle, who are capable of causing unintentional incidents that can have adverse national impacts. *Natural* threats, such as biological, seismic, meteorological, or celestial events, could also cause disruption or failure of the supply chain life-cycle.

As noted in the ITSRA, natural threats to the IT Sector are more accurately assessed via scenario models versus the use of attack trees; however, there are some general threat considerations that can be evaluated, such as assessing the severity of a storm or earthquake at a particular location.

IT Sector partners created attack trees for each of these two risks. It should be noted that the vulnerabilities they identified in each (seen in the figures below) are identical, both to each other and to the vulnerabilities identified in Section 3.1.1 for the risk of an untrustworthy product or service.

Figure 6: Distribution Failure Attack Tree

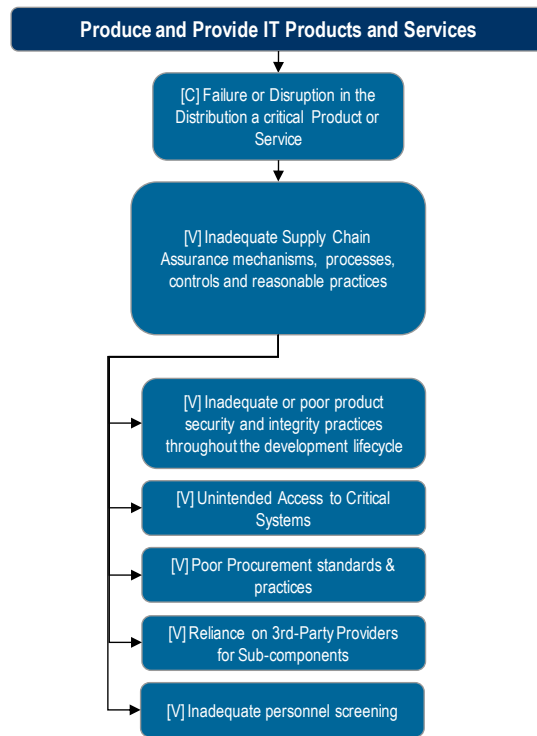
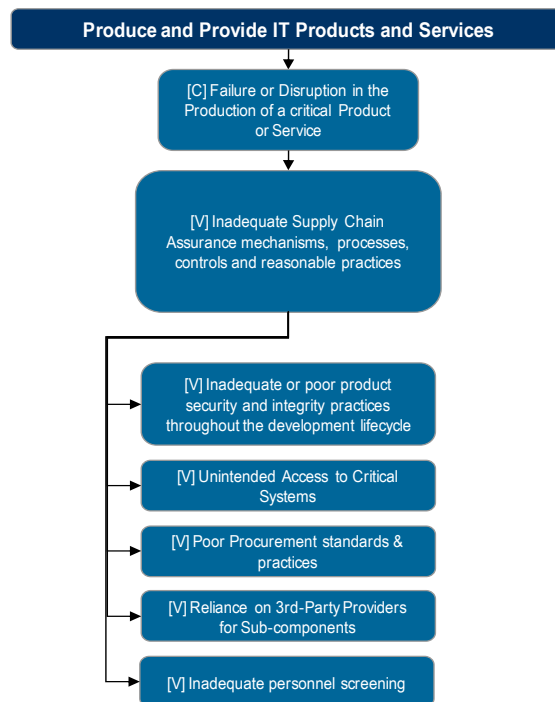


Figure 7: Production Failure or Disruption Attack Tree



3.2.2 Risk Response

Because the vulnerabilities identified for all three risks were identical, the IT Sector partners noted that the same risk mitigation strategies developed for the risk of an untrustworthy product or service are also the mitigation activities that would apply to these two risks (distribution and production failure or disruption) as well. Therefore, the partners did not develop separate risk mitigation activities for these two risks.

As before, the mitigation activities would have the same effect – namely, the likelihood would be lowered, but not enough to change the rating from “low” to “negligible,” and the consequence rating would remain “medium.”

Table 5 shows the result of applying the identified mitigations to these risks.

Table 5: Risk and Mitigation Overview

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings ¹³
Distribution Failure or Disruption	Low likelihood; low consequence	<ul style="list-style-type: none"> <input type="checkbox"/> Develop, establish, and/or adopt IT Sector standards and/or best practices <input type="checkbox"/> Use established standards and best practices to establish acquisition practices to articulate specific requirements and monitoring practices for product components and raw materials development, delivery, and integration 	Low likelihood; low consequence ¹⁴
Production Failure or Disruption	Low likelihood; medium consequence	<ul style="list-style-type: none"> <input type="checkbox"/> Enhance supply chain delivery mechanisms to minimize counterfeiting and tampering, such as implementing point verification along the supply chain (e.g., radio-frequency identification (RFID) or holograms) and using anti-counterfeiting techniques to ensure authenticity of system and network components <input type="checkbox"/> Increase awareness among the acquirers and suppliers of IT products and services of need to manage business risk, including for natural disasters, supply chain intrusion/insertion, and anti-counterfeiting 	Low likelihood; medium consequence

¹³ Assumes complete implementation of the items noted in the Risk Mitigation Activities column

¹⁴ While the overall resulting risk and consequence ratings remain the same, implementing the risk mitigation activities does lower the likelihood of a threat exploiting the vulnerability; the consequence remains unchanged. For more details, refer to 3.1.2.