Information Technology Sector Baseline Risk Assessment

August 2009

Homeland Security

IT SCC Information Technology Sector Coordinating Council

IT GCC Information Technology Government Coordinating Council

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Sector Baseline Risk Assessment	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Department of Homeland Security,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**114**	

Table of Contents

List of Figures

Executive Summary

The Information Technology (IT) Sector provides both products and services that support the efficient operation of today's global information-based society. These products and services are integral to the operations and services provided by other critical infrastructure and key resource (CIKR) sectors.

Threats to the IT Sector are complex and varied. In addition to the risks presented by natural hazards—such as catastrophic weather or seismic events—the IT Sector also faces threats from criminals, hackers, terrorists, and nation-states, all of whom have demonstrated a varying degree of capabilities and intentions to attack critical IT Sector functions. Additionally, manmade threats to the IT Sector are also rapidly evolving from simple automated worms and viruses to complex social engineering attacks that exploit known and unknown vulnerabilities in products and services developed by the IT Sector.

While existing security and response capabilities mitigate many of these threats, the IT Sector still faces Sector-wide risks to its ability to provide hardware, software, and services to other CIKR sectors. Due to the IT Sector's high degree of interdependency with other CIKR sectors and the continuously evolving threat landscape, assessing vulnerabilities and estimating consequence is difficult. Therefore, these issues must be dealt in a collaborative and flexible framework that enables the public and private sectors to enhance the resiliency and security of the critical IT Sector functions.

The IT Sector Baseline Risk Assessment evaluates risk to the IT Sector and focuses on critical IT Sector functions.[1] The assessment methodology is not intended to be guidance for individual entities' risk management activities. Instead, the IT Sector's Baseline Risk Assessment is intended to provide an all-hazards risk profile that IT Sector partners can use to inform resource allocation for research and development and other protective program measures to enhance the security and resiliency of the critical IT Sector functions. By increasing the awareness of risks across the public and private sector domains, the Baseline Risk Assessment serves as a foundation for ongoing national-level collaboration to enhance the security and resiliency of the critical IT Sector functions.

Critical IT Sector Functions

- Produce and 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

Figure 1: Critical IT Sector Functions

The risk assessment is a baseline of national-level risk since this is an initial effort to assess IT Sector risks across all six critical functions. The assessment addresses those operational or strategic risks to the IT Sector infrastructure that are of national concern based upon the knowledge and subject matter expertise of those participating in the Sector's risk assessment activities. This assessment does not address all threat scenarios faced by IT Sector entities or their users and customers. As noted in the assessment, there are areas that require additional collaborative study and further review. The document also presents potential mitigation strategies. These potential strategies are the activities that could be considered for implementation; they are not intended to name or mandate the establishment or enhancement of specific public or private sector programs.

[1] Functions are sets of processes that produce, provide, and maintain products and services. The critical IT Sector functions encompass the full set of processes involved in transforming supply inputs into IT products and services, and these processes include research and development, manufacturing, distribution, upgrades, and maintenance. The critical functions support the IT Sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered.

The IT Sector Baseline Risk Assessment was launched in September 2008 and consisted of three phases—(1) attack tree development;[2] (2) risk evaluation;[3] and (3) analysis and reporting.[4] Prior to embarking on the Baseline Risk Assessment, IT Sector partners collaboratively developed the risk assessment methodology from May 2007 through September 2008, leveraging input from private and public sector partners, as well as recognized standards and guidance organizations.

During the Baseline Risk Assessment process that began in September 2008, attack trees were developed to scope the assessment. These attack trees provided the basis for evaluation of risk to the critical functions. The subject matter experts (SME) used virtual collaboration tools and a series of meetings to develop attack trees that identified the undesired consequences for each critical function and the associated vulnerabilities and threats, where possible, that aligned to the undesired consequences.

The attack tree development phase, which concluded in October 2008, was followed by the risk evaluation phase in November and December 2008. Like the attack tree development phase, risk evaluations were conducted through a series of virtual meetings. During these sessions, the SMEs evaluated the threats, vulnerabilities, and consequences of the attack trees using the Sector's risk assessment methodology. The SMEs provided descriptions of the functions' threats, vulnerabilities, and consequences, and where appropriate, they also rated associated risk using criteria and a common scale (i.e., Negligible, Low, Medium, and High).[5] The results from the evaluation session served as the basis for the third and final phase of the assessment: analysis and reporting. To inform the Sector's risk management activities, priorities were developed collaboratively throughout the IT Sector Baseline Risk Assessment by public and private sector partners.

Since the IT Sector is globally interconnected, risk mitigations outlined in this baseline risk assessment takes into account the global and dynamic nature of IT. The critical IT Sector functions are not limited by geographic or political boundaries, increasing the need for international collaboration and coordination for risk management activities. Further study and collaboration is warranted to fully leverage existing international information sharing and security mechanisms.

The following table highlights the IT Sector's high consequence risks. These risks were identified by SMEs in a collaborative and iterative process that consisted of attack tree development, risk evaluation, and final analysis. The items captured in the *Risks of Concern* column of the table highlight the risks of greatest concern to the confidentiality, integrity, or availability impacts of the critical function. The *Mitigations* column is a summary of the mitigations identified within the function's analysis section that address the highlighted risks.

[2] Attack trees are hierarchical network diagrams that include the undesirable national-level consequences that could disrupt or degrade the six critical functions, the vulnerabilities that can be exploited to cause those undesirable consequences, and possible threats that can exploit those vulnerabilities. Each branch of an attack tree describes how a function can be destroyed, incapacitated, exploited, or diminished.
[3] Throughout this process, subject matter experts followed the IT Sector's risk assessment methodology, which was also developed by subject matter experts from across the critical IT Sector functions.
[4] Risk assessment participants developed attack trees for each critical IT Sector function. Each attack tree's top-level node(s) described the undesired consequences to the critical function, and the subsequent nodes articulated the vulnerabilities and threats that could cause the undesired consequences.
[5] Please see Appendix 3 for details about the criteria evaluated and how they relate to the common scale.

Critical IT Sector Function	Risks of Concern	Mitigations (Existing, Being Enhanced, or Potential Future)
Produce and Provide IT Products and Services	❑ Production or distribution of untrustworthy critical product/service through a successful manmade deliberate attack on a supply chain vulnerability *(Consequence: High; Likelihood: Low)*	❑ Supply chain resiliency though redundancy and process controls - *Existing Mitigation* ❑ Sourcing strategies (i.e., careful monitoring of the availability and quality of critical raw materials) - *Existing Mitigation* ❑ Product recall informed by situational awareness and timely response to compromised production - *Existing Mitigation*
Provide Domain Name Resolution Services	❑ Breakdown of a single interoperable Internet through a manmade attack, and resulting failure of governance policy *(Consequence: High; Likelihood: Medium)* ❑ Large scale manmade Denial-of-Service attack on the DNS infrastructure *(Consequence: High; Likelihood: Low)*	❑ Processes that enhance quality assurance and ensure continuous monitoring of Domain Name System (DNS) infrastructure - *Existing Mitigation* ❑ Provisioning and the use of Anycast - *Existing Mitigation* ❑ Infrastructure diversity and protection enhanced redundancy and resiliency - *Mitigation Being Enhanced*
Provide Internet-based Content, Information, and Communications Services	❑ Manmade unintentional incident caused in Internet content services result in a significant loss of e-Commerce capabilities (Consequence: High; Likelihood: Negligible)	❑ Policy and access controls - *Existing Mitigation* ❑ Security training for users and small businesses - *Mitigation Being Enhanced* ❑ Enhance rerouting capabilities of the Communications and IT Sectors - *Potential Future Mitigation*
Provide Internet Routing, Access and Connection Services	❑ Partial or complete loss of routing capabilities through a manmade deliberate attack on the Internet routing infrastructure *(Consequence: High; Likelihood: Low)*	❑ Enhanced routers (i.e., increased speed, reliability, and capacity of routers and router software) - *Existing Mitigation* ❑ Responsiveness to increasing Internet traffic - *Mitigation Being Enhanced* ❑ Increase physical security of Network Access Points and Internet Exchange Points - *Mitigation Being Enhanced* ❑ Improved incident response including contingency planning, training, and investment to enable skilled technicians to monitor networks to identify and respond to anomalies, outage, or incident - *Mitigation Being Enhanced*

Critical IT Sector Function	Risks of Concern	Mitigations (Existing, Being Enhanced, or Potential Future)
Provide Incident Management Capabilities	❑ Impact to detection capabilities due to lack of data availability resulting from a natural threat *(Consequence: High; Likelihood: Medium)*	❑ National-level incident response and coordination capabilities - *Existing Mitigation* ❑ Infrastructure and workforce diversity - *Existing Mitigation* ❑ Information sharing enhancements creating common situational awareness - *Existing Mitigation*

Figure 2: IT Sector's High Consequence Risks

In the process of conducting the IT Sector Baseline Risk Assessment, public and private IT Sector partners recognized that there were several areas for additional exploration that may have implications for the IT Sector's risk profile. These areas include:

- Identity management[6]: Although digital certificates have been recognized as secure and reliable identity credentialing tools, they impose costly and complex administrative burdens on organizations that use public key infrastructure (PKI) certificates. The weakest link, which can lead to consequences throughout the function, is the issuance of secure original identity documents. Until these issues are alleviated, the high level of assurance that digital certificates provide will remain the exclusive province of organizations that have the resources to support them or that require the levels of assurance and non-repudiation that PKI can provide. Due to the need to address the security of original identity documents, the content associated with this function only highlights *potential* risks to the function; relative ratings or analyses are not provided. Instead, public and private IT Sector partners identified this as an area that requires additional study before determining the overall risk to this critical IT Sector function.

- Manmade unintentional threats: The knowledge and measurements of risks associated with manmade unintentional threats, such as accidents, is relatively less mature than those associated with manmade deliberate threats. While the IT Sector's risk assessment methodology (see Appendix 3) does include an approach to assessing risks from manmade unintentional threats, risk assessment SMEs recommended that this be studied further.

- Natural threats and the impacts to the infrastructure: Due to increased resiliency across IT Sector entities' infrastructures, most risks associated with natural threats are contained to the immediate locale or region of the incident. Additional mitigations for these risks could reduce the potential for local or regional incidents to cascade and create national-level impacts.

- Feasibility of the establishment of a national-level testing and simulation capability: Government agencies and the private sector rely on the continued operation of the Internet and its associated functions, and public and private sector partners each have important and unique roles in securing this infrastructure. While the availability of the Internet has remained relatively constant, it is recommended that the feasibility of a potential national-level testing and simulation capability be considered. The purpose of such a program or programs would be to model upgrades and

[6] Provide Identity Management and Associated Trust Support Services is one of the six critical IT Sector functions. Unlike the five functions highlighted in the table above, risk to this function was not evaluated because public and private sector partners identified this as an area that requires additional study before threats, vulnerabilities, and consequences can be assessed. The IT Sector Baseline Risk Assessment does include issues that could be considered and evaluated further when assessing risk to this function.

changes to the Internet infrastructure and to simulate the effects of those changes. Such a program would imply that there is also a collaborative body that would analyze and create guidance for proposed infrastructure changes, based on the results of tests or simulations.

- National-level cybersecurity awareness program: Most Internet users are aware that there are significant threats to Internet content and the Internet infrastructure, but they may not be sure what they can do about them. Internet service providers, DNS server operators, hardware and software vendors, identity credential providers, and network first responders are more attuned to the risks and threats their businesses face, and most take actions to secure their operations. The development of a comprehensive and nation-wide cybersecurity awareness, training, and education program could coordinate the risk mitigation efforts of product, content, and Internet service infrastructure providers with users in government, military, educational, and private sector organizations. Efforts such as National Cyber Security Awareness Month, could serve as a model to develop year-round coordinated outreach and awareness programs. The objective of these programs is to make sure that risk mitigation activities are applied consistently across the provider and user communities. Public and private sector partners should consider enhancing or supplementing these efforts.

- Cross-sector interdependency analysis: No one sector can undertake cross-sector interdependency risk mitigation efforts alone. Studying cyber interdependencies between sectors may reveal risks not being managed in the gray areas, where sector responsibilities cross into one another. Although there are ongoing efforts in this area through the Partnership for Critical Infrastructure Security and the Information Sharing and Analysis Centers, the federal government can provide much needed resources including funding and forums for public and private sectors to jointly conduct cyber interdependency analyses, share interdependency information, and address resulting areas of risk.

Consistent with its approach to date, the IT Sector will continue to mature its risk assessment and management approach and processes. Addressing the risks highlighted in this assessment will require the continued public and private sector collaboration that has facilitated the development of this assessment. Therefore, this assessment will continue to evolve and be revised as the Sector addresses these risks. In addition, the IT Sector encourages and welcomes the active participation of additional SMEs in the IT Sector's risk management efforts to continue the expansion and increase the understanding of Sector-wide risk.

1 Introduction to Information Technology Sector Critical Infrastructure Protection

Critical infrastructure and key resources (CIKR), including information technology (IT), provide the essential services that underpin American society. Natural and manmade incidents impacting the Nation's CIKR could have debilitating effects on the Nation's security and economic well-being. Given the wide array of threats to the Nation and the scope of its infrastructure, it is imperative that a risk-based approach be applied to the security of critical infrastructure.

Risk[7] results from a complex mix of deliberate and unintentional manmade and naturally occurring threats and hazards, including deliberate attacks, accidents, natural disasters, incidents from and in cyberspace, and other emergencies. Within this context, CIKR may be directly exposed to threats and hazards themselves, or indirectly exposed as a result of the dependencies and interdependencies among the Nation's critical infrastructure.

CIKR Sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Transportation Systems
- Water

Within the CIKR protection mission area, national priorities must include preventing catastrophic loss of life and managing cascading, disruptive impact on the U.S. and global economies across multiple threat scenarios. Achieving this goal requires a strategy that appropriately balances security with focused, risk-informed prevention, protection, and preparedness activities so sector partners can manage and reduce the most serious risks they face.

The 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. Under the NIPP, each CIKR sector developed and is implementing a Sector-Specific Plan (SSP) that details the application of the overall NIPP risk management framework to its sector. SSPs are designed to describe CIP efforts and priorities. Collectively, the SSPs are used to prioritize initiatives and protective measures within and across sectors. This prioritization ensures that resources are targeted to the most effective risk mitigation areas that lower vulnerabilities, deter threats, and minimize attack and incident consequences.

Protective measures include actions to mitigate the overall risk to critical assets, systems, networks, functions, or their links, resulting from exposure, injury, destruction, incapacitation, or exploitation. This includes actions to deter the threat, mitigate vulnerabilities, and minimize consequences associated with natural and manmade threats. The IT Sector's protection efforts incorporate a holistic approach to evaluate the human, physical and cyber elements of its critical infrastructure. Protection can include a wide range of activities, such as hardening facilities, building resiliency and redundancy, incorporating hazard resistance into initial facility design, initiating active or passive countermeasures, installing security systems, promoting workforce security programs, and implementing cybersecurity measures, among others.

1.1. Partnering for Security

The NIPP describes a sector partnership model that encourages public and private sectors to collaborate on their respective infrastructure protection activities. This collaboration is accomplished through Sector

[7] Risk is the likelihood for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its probability and the associated consequences (NIPP, 2009).

Coordinating Councils (SCC)—comprising industry and private sector partners—and Government Coordinating Councils (GCC)—comprising Federal, State, local, tribal and territorial government entities.

The IT SCC and the IT GCC are the primary bodies for communicating their respective perspectives and for developing collaborative policies, strategies, and security efforts to advance CIP. As Figure 3 illustrates, public and private sector partners bring unique capabilities to the partnership and derive unique benefits through public-private sector collaboration.

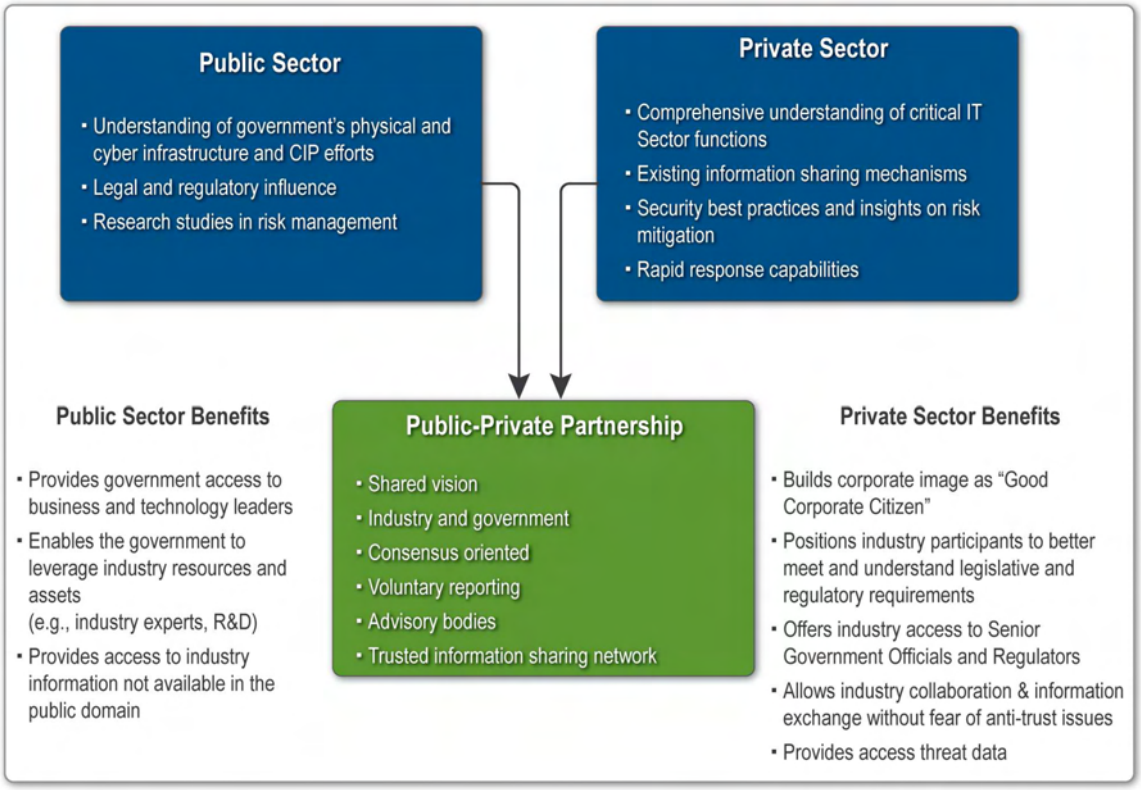


Figure 3: Benefits of Public-Private Sector Collaboration

The IT SSP, the IT SCC and GCC have contributed significant effort to the development of a credible and defensible IT Sector Baseline Risk Assessment that describes the risk to the critical functions. The following sections describe the overall IT Sector risk profile while articulating the Sector's top-down approach to assessing risk at a sector level. This assessment is unprecedented in its national-level scope and includes knowledge and expertise from across the IT Sector. This is the first IT Sector-wide risk assessment, and can inform more collaborative and synchronized management of risk in public and private sectors.

The IT SSP development and its ongoing implementation represent an unprecedented partnership and collaboration between public and private sectors as they leverage their unique capabilities to address the complex challenges of IT infrastructure protection. The IT Sector is central to the Nation's security, economy, and public health and safety. The IT Sector: provides an infrastructure upon which other CIKR sectors rely; coordinates with other CIKR sectors; and works to ensure that any disruptions or manipulations of critical functions are brief, infrequent, manageable, geographically isolated, and minimally detrimental to the welfare of the United States. Businesses, governments, academia, and private citizens are increasingly dependent upon IT Sector functions. The virtual and distributed functions evaluated in this assessment produce and provide hardware, software, and IT systems and services, and—in partnership with the Communications Sector—the Internet. As identified in the IT SSP, the six critical IT Sector functions are:

- Produce and 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; and
- Provide Internet routing, access, and connection services.

The critical functions are distributed across a broad network of infrastructure, managed on a proactive basis, and largely resilient in the face of most threats.[8] In addition, they are provided by a combination of entities—often owners and operators and their respective associations—who provide hardware, software, IT systems, and services.[9] IT Sector entities include the following:[10]

In the 2007 IT Sector-Specific Plan, the IT Sector committed to the completion of a collaborative and Sector-wide baseline risk assessment.

- Domain Name System (DNS) root and generic Top Level Domain (gTLD) operators;
- Internet Service Providers (ISP);
- Internet backbone providers;
- Internet portal and e-mail providers;
- Networking hardware companies (e.g., fiber-optics makers and line acceleration hardware manufacturers) and other hardware manufacturers (e.g., personal computer (PC) and server manufacturers);
- Software companies;
- Security services vendors;
- Communications companies that characterize themselves as having an IT role;
- IT edge and core service providers; and
- IT system integrators.

In addition, Federal, State, and local governments are a component of the IT Sector as providers of government IT services that are designed to meet the needs of citizens, businesses, and employees.

1.2. IT Sector Profile

The IT Sector Baseline Risk Assessment is a key foundation for the Sector's risk management activities. Both public and private sector partners collaborate to enhance the resiliency of the critical functions, and their expertise is reflected in this assessment. The Sector-wide risk approach evaluates risk across the Sector by focusing on critical functions; the assessment is not intended to conflict with individual entities' risk management activities. The Baseline Risk Assessment is intended to provide an all-hazards risk profile, inform resource allocation for IT Sector protection and management of its inherent risks, and increase awareness of risk across public and private sectors.

Since this is an initial effort to assess IT Sector risks across all six critical functions, the risk assessment represents a baseline of national-level risk. The assessment addresses those operational or strategic risks to the IT Sector infrastructure that are of national concern based upon the knowledge and subject matter expertise of those participating in the Sector's risk assessment activities. This assessment does not address all threat scenarios faced by IT Sector entities or their users and customers. As noted in specific sections of the assessment, there are areas that require additional collaborative study and further review. The assessment also presents potential mitigation strategies. The strategies outlined are

[8] Threat is defined as the natural or manmade *incidents* (intentional or unintentional) that would be detrimental to the IT Sector.
[9] IT services include development, integration, operations, communications, and security.
[10] Operating Charter of the Information Technology Sector Coordinating Council, September 19, 2008 https://www.it-isac.org/documents/itscc/index.php

potential solutions requiring more intense scrutiny and thought, which is beyond the scope of this assessment.

Enhancing the resiliency and security of the IT Sector's critical functions is a shared responsibility of government and industry. The IT Sector Baseline Risk Assessment highlights overarching areas wherein implementing identified mitigations will assist the sector to enhance its resiliency. Public and private sector representatives from the IT Sector have established a process for informing R&D programs and other risk mitigation activities within and across the public and private sectors. This collaborative process will be used to address the risks of concern that are identified in this assessment.

2 Risk Management Approach, Methodology, and Process

The IT Sector's risks are inherently complex and dynamic. However, a few primary characteristics shape the evolving risk environment:

- Significant interdependencies exist between the IT Sector and other CIKR sectors;
- The highly diverse, virtual, interconnected, and international nature of the IT infrastructure; and
- The constantly evolving threat landscape.

Individual IT Sector entities manage risk to their own infrastructures, and as articulated throughout this assessment, the IT Sector engages in risk management activities at the national- and sector-levels. This section articulates the Sector's risk approach as well as the methodology and process used to define its baseline risk profile.

Critical IT Sector functions are provided by a combination of entities—often owners and operators and their respective associations—who provide hardware, software, IT systems, and services.

The IT Sector has global operations that are interdependent and connected with other infrastructures. These operations enhance efficiency and effectiveness and increase the resilience of the Sector; however, they face numerous multifaceted global threats from natural and manmade events on a daily basis. Many of these events occur frequently, but do not have significant consequences because of individual entities' existing security and response capabilities. However, some of these threats are strategic and could affect critical functions and other elements of the Nation's critical infrastructure. The high degree of the IT Sector's interdependency and interconnectedness as well as anonymity of actors, makes identifying threats, assessing vulnerabilities, and estimating consequence difficult. Therefore, they must be dealt with using a collaborative and innovative approach.

2.1. Assessing Risk at a Sector-level

A national-level understanding of risk by both public and private sector partners informs policies for risk mitigation and informs resource allocation for research and development (R&D) activities. This national-level perspective complements and elevates the positive impacts of individual entities' risk management efforts. The IT Sector applied a top-down and functions-based approach that considers the Sector's ability to support the economy and national security as part of the risk assessment's national-level scope. Figure 4 provides a summary of the methodology used to gain subject matter experts' insights regarding Sector-wide risks.[11] The details that support each element and component of the methodology can be found in Appendix 3.

[11] The methodology was developed by IT Sector partners as articulated in the IT SSP. The development of this methodology was necessary given the national- and sector-level approach detailed in the IT SSP. The methodology leverages the knowledge and expertise of IT Sector partners, standards and guidance bodies, and other credible authorities in the IT, risk management, and critical infrastructure protection arenas.

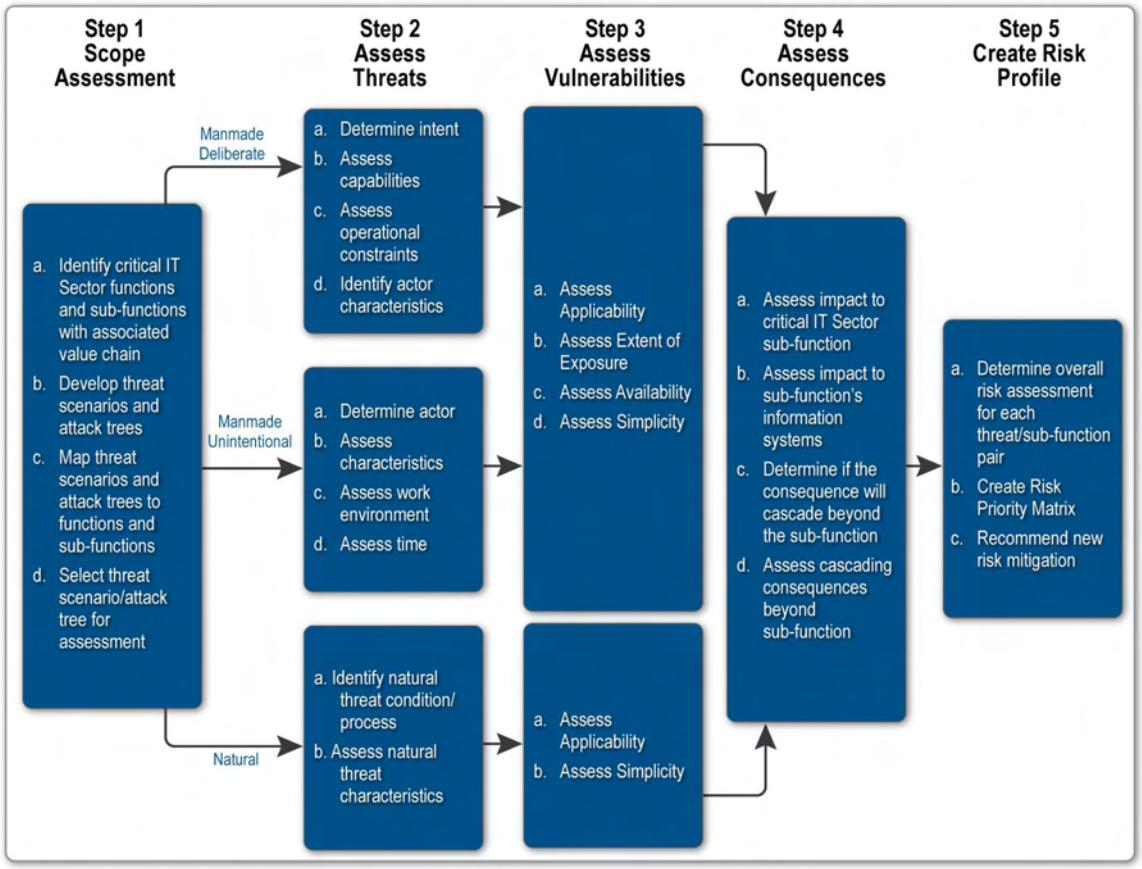


Figure 4: IT Sector Risk Assessment Methodology

The IT Sector's risk approach evaluates risk across the Sector by focusing on critical functions rather than specific organizations or assets. In addition, risk management approaches used by individual entities are generally based on various philosophies, methodologies, and tools.[12] Private sector entities typically base their approaches on business objectives, such as shareholder value, efficacy, and customer service. Regulatory compliance requirements associated with financial reporting integrity and privacy initiatives are other practices that impact risk management strategies.

2.2. Identifying Critical Functions

Functions are sets of processes that produce, provide, and maintain products and services. The functions encompass the full set of processes involved in transforming supply inputs into IT products and services, such as research and development (R&D), manufacturing, distribution, upgrades, and maintenance. These functions support the Sector's ability to produce and provide high-assurance products, services, and practices that are resilient to threats and can be rapidly recovered. Assurance is essential to achieving the Sector's vision and is therefore a fundamental aspect of all critical functions. The functions are not limited by geographic or political boundaries, increasing the need for international

[12] IT Sector entities assess various types of risk (e.g., financial, human, supply chain, legal, and compliance) through multiple approaches (e.g., quantitative, qualitative, and modeling and simulation), leveraging both commercial and government off-the-shelf products and customized tools. These entities use a variety of common risk management frameworks to proactively manage steady-state risk. These individual risk management efforts are designed to support organizational business objectives and, in aggregate, they enhance the security and resilience of the Sector as a whole.

collaboration and coordination for risk assessment activities, best practices, and protective program design and implementation. The infrastructure's distributed nature inherently provides physical and virtual resilience; however, some functions may have supporting infrastructure with less than sufficient resiliency, which could present risk and potentially increase their vulnerability.

The purpose of utilizing a top-down approach to assessing functions is to identify those functions that meet a minimum consequence threshold primarily based on resiliency.[13] Resources can then be devoted to analyzing nationally consequential functions and their supporting infrastructure. IT Sector functions have been screened and prioritized based on Homeland Security Presidential Directive 7 (HSPD-7) consequence categories and criteria for evaluating nationally significant events. These criteria are included below and the IT Sector's consequence framework—described in Section 2.4.3, Evaluating Consequences—provides insight to the threshold or additional factors considered when assessing overall risk to the critical functions.[14]

- Governance Impact: Effects on Federal, State, and local governments;
- Economic Security Impact: Effects on the users and greater economy;
- Public Health and Safety Impact: Effects on human health by injuries and loss of life; and
- Public Confidence Impact: Effects on the public's morale caused by the visibility of the impact, the number of people affected, and the length of time needed to switch to alternative sources.

Figure 5 identifies and describes the critical IT Sector functions, each of which impact the consequence factors defined above. These functions are required to maintain or reconstitute the network (e.g., the Internet, local networks, and wide area networks) and its associated services. The list represents IT SCC and GCC consensus on critical functions that are vital to national and economic security and public health, safety, and confidence.

[13] The IT Sector functions' criticality is assessed based on their potential impact on government or sector missions, independent of any specific defined threat scenario. A function's criticality depends on many factors, such as tolerable magnitude and duration of loss or degradation of a particular function. The resilience of functions to disruption or degradation increases with the availability of substitutes for the products and services, resulting from a given critical function with the degree of diversity that exists within the functions' processes and with diversity of providers. A disruption or degradation of a function can have a cascading effect, if other functions are highly dependent on its outputs. Functions with high dependence and interdependence are of particular concern in this assessment.

[14] IT Sector subject matter experts collaboratively developed the consequence thresholds based upon the general categories identified in HSPD-7. The details of the IT Sector's consequence framework can be found in Appendix 3.

IT Sector Function	Description
Provide IT Products and Services	The IT Sector conducts operations and services that provide for the design, development, distribution, and support of IT products (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 hardware and software products and services are limited to those necessary to maintain or reconstitute the network and its associated services.
Provide Incident Management Capabilities	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.
Provide Domain Name Resolution Services	The IT Sector provides and operates domain registration services, top-level domain (TLD)/root infrastructures, and resolution services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Identity Management and Associated Trust Support Services	The IT Sector produces and provides technologies, services, and infrastructure to ensure the identity of, authenticate, and authorize entities and ensure confidentiality, integrity, and availability of devices, services, data, and transactions that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet-based Content, Information, and Communications Services	The IT Sector produces and provides technologies, services, and infrastructure that deliver key content, information, and communications capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.
Provide Internet Routing, Access, and Connection Services	The IT Sector (in close collaboration with the Communications 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.

Figure 5: Critical IT Sector Functions and Descriptions

In addition to identifying the functions in Figure 5, the Sector defined critical sub-functions that represent those operations and processes that support each function. For the purposes of the Baseline Risk Assessment, IT Sector SMEs evaluated and articulated risks at the function-level, although, in some cases, a limited number of sub-functions were analyzed. As the Sector's risk management process matures or is modified, specific and relevant sub-functions may be evaluated.

2.3. Developing Attack Trees

Public and private sector partners created attack trees[15] in function-specific working groups to characterize risks to the critical functions. The attack trees and their identified threats, vulnerabilities, and consequences formed the basis of the risk description and evaluation of IT Sector risk. The attack trees developed for each critical function follow a common framework that consists of:

- Capturing a limited number of potentially nationally significant undesirable consequences;
- Identifying vulnerabilities that could cause the undesirable consequences; and
- Characterizing threats that could exploit the vulnerabilities.

After building the attack trees for each of the six critical functions, SMEs identified branches of each tree to assess. In assessing each branch, SMEs focused on identifying:

[15] Attack trees are hierarchical network diagrams that include the undesirable national-level consequences that could disrupt or degrade the six critical functions, the vulnerabilities that can be exploited to cause those undesirable consequences, and possible threats that can exploit those vulnerabilities. Each branch of an attack tree describes how a function can be destroyed, incapacitated, or exploited.

- First-order consequences to the function (e.g., describing the function's impacts according to the criteria of confidentiality, integrity, availability;
- Vulnerabilities that are exploited to achieve selected consequences; and
- Threat capabilities and resources necessary to exploit vulnerabilities, which is an optional element in some attack trees and branches.

2.4. Identifying and Measuring Risk

The risk assessment approach evaluates threats to the critical functions; associated vulnerabilities and consequences identified in the attack tree; considers the effectiveness of mitigations that are already in place; and proposes new or enhanced capabilities needed to effectively manage risk. To provide comparable results among and across the function-level analyses, consistent ratings and measurements are used for evaluating threats, vulnerabilities, consequences, and mitigations. These ratings are accompanied by descriptions of threats, vulnerabilities, consequences, and mitigations to develop the IT Sector's overall risk profile.

Private sector entities implement mitigations primarily based on their organizational objectives and operations, whereas public sector interests are focused on assuring the ability of critical functions to support national and homeland security, economic security, public health and safety, and public confidence. Understanding how existing public and private sector risk mitigations complement each other to collectively address risks and identifying additional capabilities is an essential component of the risk management approach. These complementary mitigations and additional capabilities are considered as part of the IT Sector's process for identifying and implementing new protective programs or R&D initiatives. Throughout the risk assessment methodology, existing mitigations are considered and identified.

Because limited resources exist to manage the wide range of risks, it is important that public and private sector partners agree on how to best prioritize risks and apply resources to ensure that critical functions are protected. Sector-wide risk management activities focus on mitigating, transferring, or accepting risks. At the national-level, public policy can also be influenced. In addition, incentives can be developed for private sector entities to encourage them to consider a more robust national or Sector-wide perspective in their risk management activities.

2.4.1 Analyzing Threats

The IT Sector's threat analysis approach considers the full spectrum of manmade (intentional and unintentional) and natural threats. Due to the different intrinsic qualities of manmade deliberate, manmade unintentional, and natural threats, the risk assessment methodology includes unique, but comparable, components for analyzing these threats and assessing their associated vulnerabilities. These factors flow into a common consequence evaluation for all threats to the critical functions.

For manmade deliberate threats, traditional threat analysis generally identifies an actor and the actor's intentions, motives, and capabilities to compromise a given target. Such approaches typically rely on historical data, current intelligence, and analysts' speculation associated with a particular actor to predict threats. When analyzing threats to the IT Sector, this traditional approach to threat assessment alone is not sufficient in the Sector's risk environment because actors are not easily identifiable or traceable, and attacks—deliberate or unintentional—can go from conception to exploitation within hours. The IT Sector's approach complements the traditional threat assessment approach by including additional factors based on capabilities and intent independent of known actors to consider emerging non-traditional threats.

The IT Sector's threat analysis approach considers threats that have national significance based on a threat's capabilities. This approach is consistent with traditional threat analysis approaches, which typically focus on specific actors and then evaluate their capabilities. Due to the difficulty with identifying threat actors, especially in cyberspace, the IT Sector focuses on a threat's capabilities to exploit vulnerabilities before identifying specific actors.

The Sector defines threat capability as the availability and/or the ease of use of tools or methods that could potentially be used to damage, disrupt, or destroy critical functions. With respect to natural threat, capability is inherent; therefore, natural threats that could have a nationally significant impact will be considered. A capabilities-based approach is applied differently for intentional manmade threats. For intentional manmade threats, widely available tools or methods that can be easily configured to exploit critical functions present significant challenges. The IT Sector is also vulnerable to unintentional manmade threat because of its high reliance on human interaction and skill sets.

Threat Categories

- The **manmade deliberate** threat component focuses on incidents that are either enabled or deliberately caused by human beings with malicious intent. It facilitates a qualitative assessment of these threats by analyzing their intent and capabilities and identifying the actors' characteristics.
- The **manmade unintentional** threat component focuses on incidents that are enabled or caused by human beings without malicious intent. It facilitates a qualitative assessment of these threats by analyzing the inherent qualities of actors and the work environment.
- The **natural** threat component focuses on non-manmade incidents caused by biological, geological, seismic, hydrologic, or meteorological conditions or processes in the natural environment. It leverages existing measurement scales from recognized organizations (e.g., the National Oceanic and Atmospheric Administration, the Federal Emergency Management Agency, and the Centers for Disease Control) to identify and measure the severity and likelihood of natural threats to affect the critical IT Sector functions and sub-functions.

2.4.2 Assessing Vulnerabilities

The vulnerability analysis approach considers the people, process, technology, and physical vulnerabilities that, if exploited, could impact the confidentiality, integrity or availability of critical functions. The approaches for assessing vulnerabilities for manmade deliberate and unintentional threats are similar and use four consistent criteria: applicability, extent of exposure, availability, and simplicity. The factors associated with each threat type vary slightly, as shown in Figure 6, since extent of exposure and availability are not measurable factors when assessing vulnerabilities to natural threats. Also, the vulnerability factors determine the nature of vulnerability within the infrastructure in isolation (simplicity and availability) and the relationship between the threat and the vulnerability (applicability and extent of exposure).

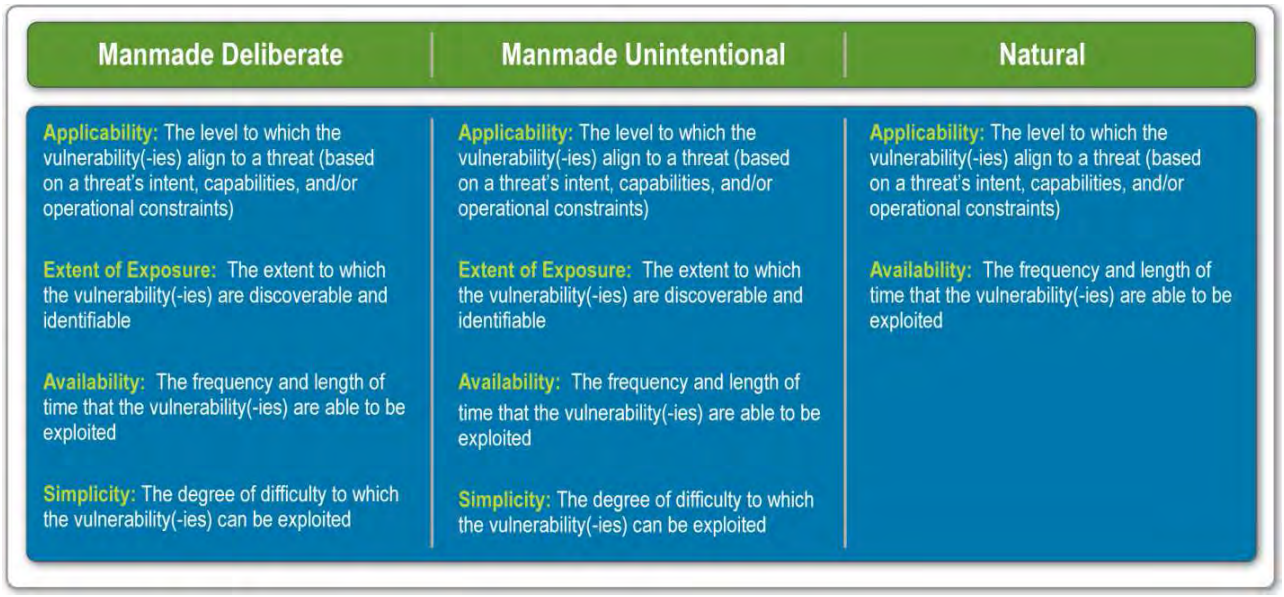


Figure 6: IT Sector Risk Assessment Methodology Vulnerability Factors

2.4.3 Evaluating Consequences

The consequence framework is common to all threat types. The framework assesses the first order impacts to the confidentiality, integrity, and/or availability of the critical functions, as well as second order impacts that cascade to users that rely on the critical functions and sub-functions using the four consequence factors derived from HSPD-7.

The potential consequences associated with nationally significant events represent the expected range of direct and indirect impacts that can occur should a threat exploit vulnerabilities in critical functions. The interdependency between the physical and cyber elements of the infrastructure must also be considered when assessing risk. Therefore, the Sector's approach to consequence assessment identifies impacts on national and economic security and public health, safety, and confidence should a critical function be disrupted or degraded.

2.5. Developing the Baseline Risk Profile

The IT SSP, published May 2007, established a collaborative public-private working group to guide and facilitate implementation of the risk management actions from the SSP and conduct a baseline risk assessment to initiate management of Sector-wide risk. Many of the risk management actions from the IT SSP focused on efforts to refine the approach outlined in the SSP and initiate the identification of threats, vulnerabilities, and consequences. The IT Sector refined the top-down and functions-based approach described in the IT SSP into a methodology, which can be found in Appendix 3. After refining the IT Sector risk assessment methodology, the IT Sector conducted a pilot risk assessment in March 2008 to validate the accuracy and usability of the IT Sector risk methodology and test the process for conducting the assessment. The lessons learned from the pilot risk assessment were then prioritized and incorporated into the IT Sector risk methodology. Prior to embarking on the Baseline Risk Assessment, IT Sector partners collaboratively developed the risk assessment methodology from May 2007 through September 2008. The IT Sector Baseline Risk Assessment was launched in September 2008 and consisted of three phases—(1) attack tree development; (2) risk evaluation; and (3) analysis and reporting.

In March 2008, the IT Sector conducted a pilot assessment to determine the accuracy and usability of the IT Sector risk methodology.

During the Baseline Risk Assessment process that began in September 2008, attack trees were developed to scope the assessment. These attack trees provided the basis for evaluation of risk to the critical functions. The SMEs used virtual collaboration tools and a series of meetings to develop attack trees that identified the undesired consequences for each critical function and the associated vulnerabilities and threats, where possible, that aligned to the undesired consequences.

The attack tree development phase, which concluded in October 2008, was followed by the risk evaluation phase in November and December 2008. Like the attack tree development phase, risk evaluations were conducted through a series of virtual meetings. During these sessions, the SMEs evaluated the threats, vulnerabilities, and consequences of the attack trees using the Sector's risk assessment methodology. The SMEs provided descriptions of the functions' threats, vulnerabilities, and consequences, and where appropriate, they also rated associated risk using criteria and a common scale (i.e., Negligible, Low, Medium, and High).[16]

The results from the evaluation session served as the basis for the third and final phase of the assessment: analysis and reporting. Throughout each of the phases, SMEs provided insights to national- and sector-level risks to the critical functions, thus making this assessment a collaborative and iterative process that involved public and private sector partners. To inform the IT Sector's risk management activities, priorities were developed collaboratively throughout the Baseline Risk Assessment by public and private sector partners.

[16] Please see Appendix 3 for details about the criteria evaluated and how they relate to the common scale.

3 IT Sector Baseline Risk Profile[17]

This section provides the risk profile for the critical functions and concludes with an overview of cross-function interdependencies and IT Sector dependencies. Sections 3.1 through 3.6 illustrate each function's risk profile in a common format, which begins with a summary text box, a description and definition of the critical function, an overview and analysis of the function's attack tree and risk profile, and an overview of existing, enhanced, and potential future mitigations. Each section's summary box includes a table depicting the relative risk associated with the main components of each function's attack tree. These relative risk tables are intended to drive the prioritization of risk assessment activities and highlight risks that the Sector should consider mitigating. Section 3.7 highlights the interdependencies across the functions and provides a relative measurement to these interdependencies. Section 3.7 also briefly notes the CIKR sector on which the IT Sector depends and how it relies on that sector.

3.1. Produce and Provide IT Products and Services

***Produce and Provide IT Products and 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 this 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;

[17] The risk assessment serves as a baseline of national-level strategic and operational risks to IT Sector critical functions based upon the knowledge and subject matter expertise of participants. As noted throughout this section, there are areas that will require additional collaborative study and further review.

- 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;[18]
- Develop and provide secure appliances that support DNS;[19] 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.

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 and 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.

The *Produce and Provide IT Products and Services* function is susceptible to a different threat landscape than other critical functions. Despite the broad scope and diversity across the sub-functions, these sub-functions are comprised of common elements, as noted in the value chain below. Due to the inherent resiliency of significant elements of the function, impacts to the availability of producing and providing IT products and services are generally managed to acceptable levels of Sector-wide risk. 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 identify 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.

[18] 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.
[19] 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.

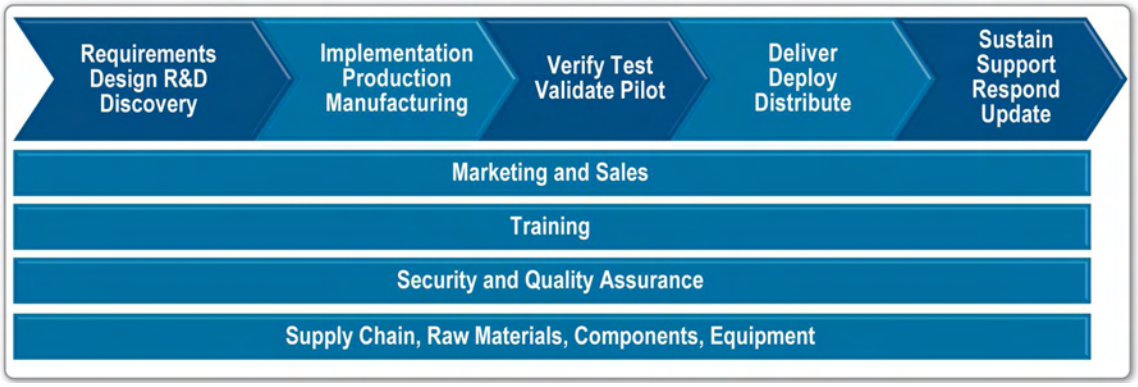


Figure 7: IT Sector Products and Services Value Chain

National-level consequences from an exploited vulnerability affecting confidentiality or integrity generally require a sustained breakdown in mitigations across the infrastructure, which the SMEs do not find very likely. Integrity and confidentiality impacts to the function can occur if a threat exploits vulnerabilities resulting from pressure to deliver low-cost products quickly, thereby forcing producers to use less effective processes for standard practices, such as vetting potential vendors. Also, the length of some supply chains can make it difficult to monitor or have robust controls at every point, providing the opportunity for a threat to exploit the supply chain. The complexity of many components increases the possibility of compound failures and the difficulty in identifying compromises so they can be mitigated. Additionally, implementation of security controls and response capabilities for these situations is more ad hoc than those for potential availability-related impacts partially due to the complex nature of the threat and vulnerability landscape. Typically, response begins with taking the affected components offline until replacements are ready; however, damage may have occurred by the time of detection, or the compromise may never be detected.

3.1.1 *Produce and Provide IT Products and Services* Attack Tree and Risk Profile

Figure 8 illustrates the scope of the assessment for *Produce and Provide IT Products and Services* function. Specifically, the function's attack tree focuses on the production, distribution, and trustworthiness of critical IT hardware, software, and services. Focusing on the production and distribution of trustworthy products, SMEs identified vulnerabilities that, if exploited, would impact the function. The attack tree identifies a variety of potential physical, people, process, and technology vulnerabilities that manmade, natural, or unintentional threats can exploit. Also, dependencies on other infrastructures can impact the IT Sector's ability to produce and distribute hardware and software. For the Baseline Risk Assessment, SMEs evaluated potential impacts from disruptions to the Water, Transportation Systems, Communications, and Energy sectors.[20] The SMEs selected these sectors because they sought to limit the Baseline Risk Assessment's scope. Section 4 of this report identifies additional sectors upon which the IT Sector relies.

[20] Dependency on the electrical grid was viewed from a U.S./Canada-centric perspective only. The Sector deemed a global perspective, at this juncture, too broad to be evaluated or assessed in an accurate manner.

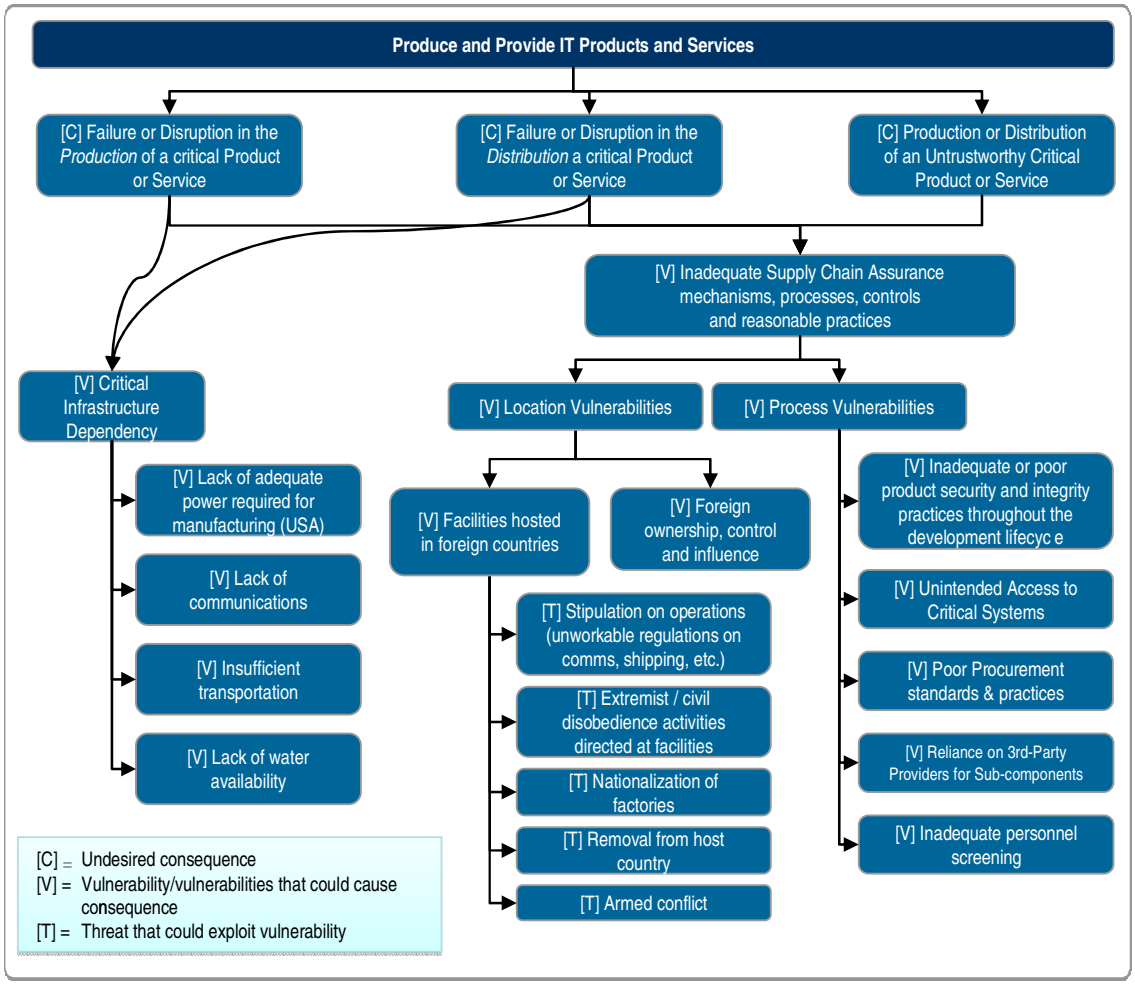


Figure 8: *Produce and Provide IT Products and Services* Attack Tree

Exploitation of IT hardware and software through counterfeiting or disruptions to the just-in-time-delivery and manufacturing aspects of the function can cause national-level impacts, despite the redundancy and resiliency of many elements of the function's supply chain.

Supply chain-related threat actors include corporate spies, corrupt government officials, cyber vandals, disgruntled employees, foreign government agents or spies, foreign military, government agent or spy, nation-states, radical activists, or criminals. Manmade deliberate threat actors can be motivated by financial gain; intelligence gathering, including state-sponsored as well as corporate espionage; the desire to project power through capability demonstrations; or to mislead consumers. Attacks against the supply chain can manifest themselves physically, such as limiting the flow of certain materials required for manufacturing hardware, and logically, such as compromising organizations' supply management processes or systems. Because cyber attacks on a supply chain typically require a higher degree of coordination and sophistication, SMEs believe that cyber attacks to the supply chain are less likely to occur relative to other types of cyber attacks to the infrastructure supporting this function as well as the other critical IT Sector functions.

Regardless of the attack method (physical or logical), most successful attacks are likely to occur covertly, making attribution difficult to ascertain. These attacks would most likely be conducted by actors who are sophisticated and well-organized and are probably associated with larger entities, such as structured organized crime syndicates and nation-states that have a financial or political interest in disrupting the

production, distribution, or trustworthiness of hardware or software. However, actors could also include individuals, such as a disgruntled employee with access to a critical process and information, but the relative consequences of an individual's or group's attack would likely be less severe than those of organizations or nation-states.

Manmade unintentional—or accidental—threats are also relevant to the supply chain of the *Produce and Provide IT Products and Services* function. Employees throughout the distribution, manufacturing, update, and sustaining aspects of the product lifecycle are capable of causing unintentional incidents that can have adverse national impacts.

Natural threats, such as biological, seismic, meteorological, or celestial events, are possible threats to the supply chain of the *Produce and Provide IT Products and Services* function. 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**.**

Due to the variety of products developed by the Sector and the global nature of these products' supply chains, limiting the availability and exposure of the function's vulnerabilities requires effective management practices for authenticity, integrity, security, and response capabilities—some of which are yet to be developed—to successfully mitigate the overall risk for this function. Single points of failure within the supply chain, where resources are concentrated, are especially relevant when assessing the overall risk to the function. For example, attacks on distribution lines will probably not impact software manufacturers as much as hardware manufacturers because software manufacturers do not solely rely on physical distribution channels (e.g., software products can be downloaded via the Internet). The ability of the Sector to provide IT products and services may be adversely impacted in the unlikely event of prolonged degradation or unavailability of part or all of the product supply chain.

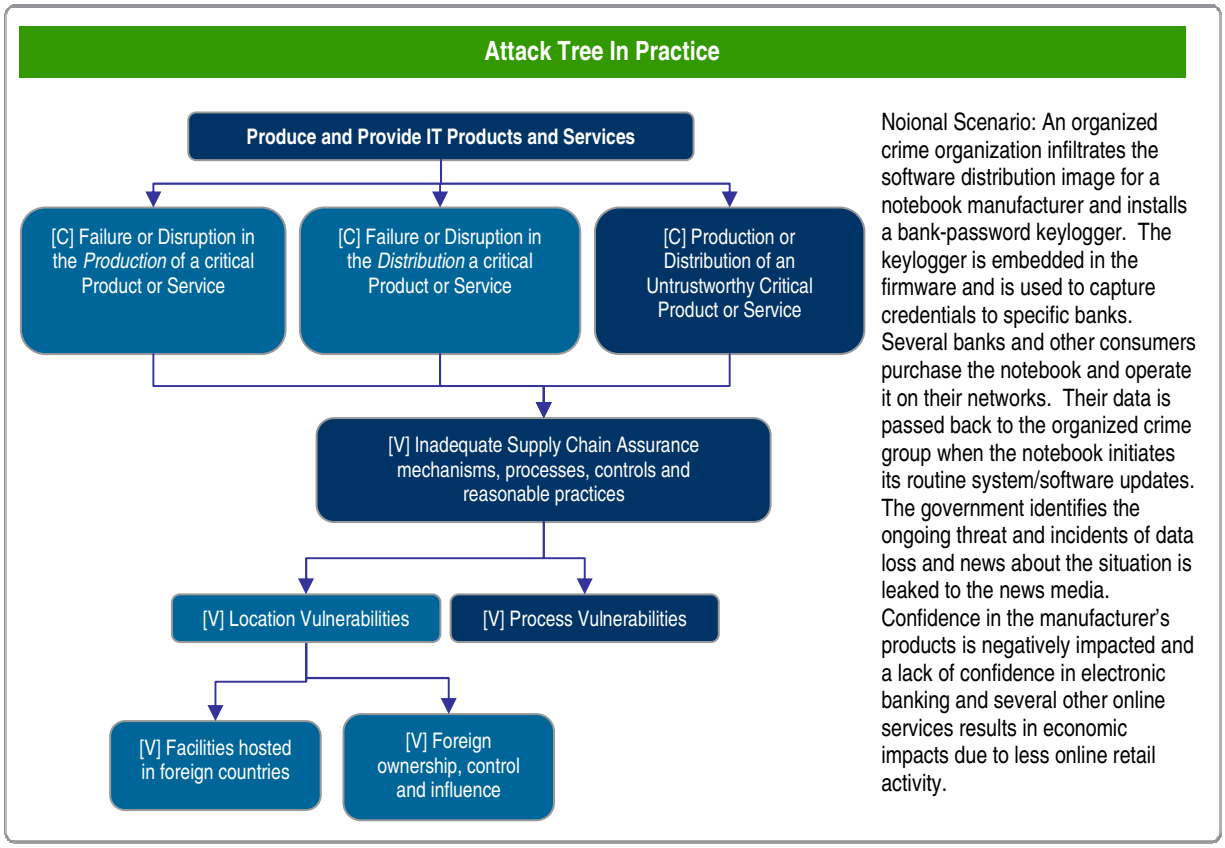


Figure 9: Notional scenario applied to the *Produce and Provide IT Products and Services* Attack Tree

Similar to the threat posed by individuals conducting deliberate attacks, significant consequences from an unintentional incident would require a sustained breakdown in mitigations across the infrastructure due to the function's redundancy in several elements of the supply chain. Examples of unintentional threats to the function include incidents caused by employees resulting from inadequate or poor product security and integrity practices throughout the development lifecycle; unintended access to critical systems; poor procurement standards and practices; reliance on third-party providers for sub-components; and inadequate personnel screening. Unintentional threats—or accidents–can produce consequences that are of national significance. If there are persistent or widespread occurrences of accidents, each of which are likely but not nationally significant, their combined effect could cause prolonged or significant impacts to the function.

The IT Sector is highly dependent on energy, communications, transportation, and water[21] critical infrastructures. Sustained interruption of any one of these infrastructures due to events outside the control of the IT Sector can cause cascading failures or disruptions in the production or distribution of critical products or services. Further cross-sector analysis is needed to determine the level of impact from a sustained outage.

Single points of failure within the supply chain are also susceptible to natural events, such as earthquakes, tsunamis, or hurricanes. There are some general vulnerability considerations that can be evaluated, such as identifying the suitable hazard conditions at or near a single point of failure location,

[21] The Water Sector was identified during the attack tree development session; data centers often use high-tonnage HVAC systems that require drinking water to operate to keep their computer systems cool; and production plants require purified potable water for the generation of steam for cogeneration of electricity and steam-driven processes.

as well as evaluating the protection and prevention measures, training, and concentration of technological and human resources at the location. Impacts to single points of failure within the supply chain can cause short-term failures or disruptions in the production or distribution of critical products and services, as well as cause the production or distribution of untrustworthy critical products or services.

Supply chain threats to the *Produce and Provide IT Products and Services* function could impact the confidentiality, integrity, and availability of the function. The complex, transitory, and global nature of the commercial IT and Communications Sectors provides opportunities for adversaries to gain unauthorized access to data, alter data, disrupt operations, or interrupt communications by inserting malicious code or otherwise corrupting components bound for U.S. systems. Specifically, the introduction of an untrustworthy product to consumers impacts the integrity and potentially the trustworthiness of the product. The tangible consequences from this could include the loss of intellectual property; identification of key personnel on projects or products; loss of brand image; possible degradation of the overall system or function being provided by multiple entities; and significant economic impacts, since the product will require repair or replacement.

A successful deliberate attack on this function could have a significant impact on the Nation's homeland and economic security, public health and safety missions, and public confidence. These consequences impact each area differently, and they are dependent on the length of disruption and could impact defense, emergency response, and law enforcement functions. Due to the global nature of the *Produce and Provide IT Products and Services* function's supply chain, at any given time, there may be many areas exposed to possible exploitation and covert attack. Therefore, monitoring of every element or node of the supply chain is difficult. Thus, consequences of the deployment or distribution of an untrustworthy product or service would most likely take weeks or months to detect and identify. Similarly, to fully recover from or reconstitute the function after an attack would probably take months.

Monitoring of every element or node of the supply chain is difficult. Consequences of the deployment or distribution of an untrustworthy product or service would most likely take weeks or months to detect and identify. Similarly, to fully recover from or reconstitute the function after an attack would probably take months.

Figure 10 summarizes the relative risk to the *Produce and Provide IT Products and Services* function. The distribution or production of an untrustworthy product or service is of greater relative concern than risks associated with the ability of the Sector to produce or distribute hardware, software, and services. In addition, at the present time, manmade deliberate threats are of greater concern than manmade unintentional threats. However, risk assessment SMEs expressed interest and concern about potential impacts of unintentional threats to the IT Sector's ability to produce and provide IT hardware, software, and services. The persistent potential threats posed by unintentional threats require discipline across entities within the Sector. This theme is also consistent across the other critical functions.

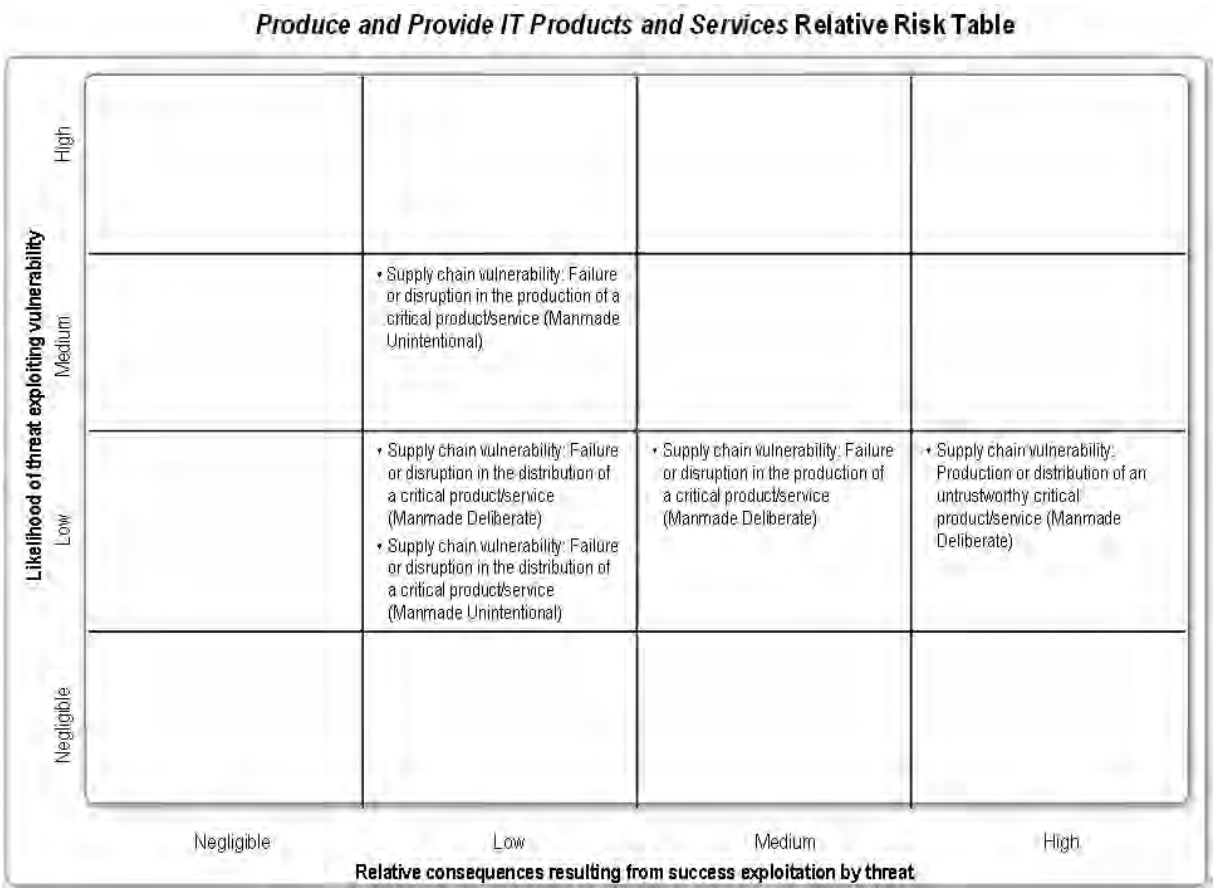


Figure 10: Relative Risks to the *Produce and Provide IT Products and Services* Function

3.1.2 Mitigations

As part of the Baseline Risk Assessment, the SMEs identified existing and future mitigations that address the risks outlined for the *Produce and Provide IT Products and Services* function. The mitigations were categorized as existing mitigations, mitigations currently being enhanced and improved, and future mitigations. These categories will assist the IT Sector outline R&D and protective program priorities.

Existing Mitigations

- Supply chain resiliency through redundancy and process controls: Many software and hardware manufacturers have redundancy throughout their supply chains, thereby preventing possible local and regional vulnerabilities from cascading to Sector-wide events. Supply chain vulnerabilities are typically mitigated by robust and repeatable controls, as well as practices and processes that include mechanisms for updates and revisions to address the changing threat landscape. These controls, practices, and processes can be unique to the particular region in which they are performed or they can be driven by the types of operations being performed. Business continuity and contingency planning also enable producers and providers to recover or reconstitute as quickly as possible in the event an attack or outage occurs.

- Sourcing strategies: An adequate supply of raw materials is essential for just-in-time manufacturing of critical IT products. The Sector carefully monitors the availability and quality of critical raw materials, and maintains sufficient inventory of these raw materials. The monitoring of stockpile inventory versus market demand to ensure material availability is typically accomplished through automated or semi-automated means.

- Product recall: Situational awareness and timely response to compromised production ensures the trustworthiness of critical IT products. Whereas a quality control program is used to prevent defects during production, a typical means of mitigating against compromised IT products after delivery is to immediately halt production and provide logistics, such as a Return Material Authorization center, to recall, replace, patch, or upgrade hardware or software.

Mitigations Currently Being Enhanced and Improved

- Ongoing efforts to enhance and refine quality assurance and quality control: Continuous and regular review, testing, and updating of software and hardware manufacturing processes make the Sector's supply chain more resilient. Capability Maturity Model Integration (CMMI) [22] and Lean Six Sigma (LSS)[23] are typical process improvement approaches that many public and private sector organizations deploy, both nationally and internationally, to improve the production, distribution, and trustworthiness.

- Building security into IT hardware, software, and services: Software assurance programs promote the reduction of software vulnerabilities through proper security coding standards, thereby minimizing exploitable weaknesses and improving the development and deployment of trustworthy software products. Software assurance mitigates people, processes, technology, and acquisition vulnerabilities. The Sector is broadly adopting software assurance processes which consider R&D, modeling and simulation, developmental and operational testing, technical analysis, and training to ensure that every stage in the development life cycle adequately and tangibly addresses security.

Potential Future Mitigations

- Increased awareness of manmade unintentional threats and mitigations to accidental risk: In part because of the human and process oriented nature of the IT Sector, products and services are prone to manmade unintentional threats. Further study and analysis is needed for industry and government to mitigate supply chain risk to unintentional threats to an acceptable level.

[22] "What is CMMI?" Software Engineering Institute, Carnegie Mellon University. 2009. http://www.sei.cmu.edu/cmmi/general/index.html
[23] "Lean Six Sigma". *Hot Topics in Quality*. American Society for Quality Knowledge Center http://www.asq.org/six-sigma/index.html

3.2. Provide Domain Name Resolution Services

Provide Domain Name Resolution Services Function Summary	
Situation	Almost all Internet communications today rely on the DNS, making it one of the most critical protocols to the IT infrastructure.
Concern	An attack that causes national-level impacts against the *Provide Domain Name Resolution Services* function would most likely be part of an attack against another element of the IT Sector infrastructure, and cause collateral damage to the DNS.
Impact	Policy and governance failures as a result of a decrease in interoperability could cause significant and lasting economic and national security consequences to the critical DNS function.

The Domain Name System, or DNS, is a hierarchy of name servers that converts and resolves contextual host and domain names into Internet Protocol (IP) addresses for every external-facing Web server, e-mail server, or other network device registered on the Internet. The DNS allows Internet users to access services, such as Web pages, e-mail, Instant Messages, and files by typing in the name for the host instead of a more difficult to remember IP address. Almost all Internet communications today rely on the DNS, making it one of the most critical protocols to the IT infrastructure. Because most end-user IPs require the ability to look up host names and addresses, the DNS is as critical to the Internet as data transmission lines.

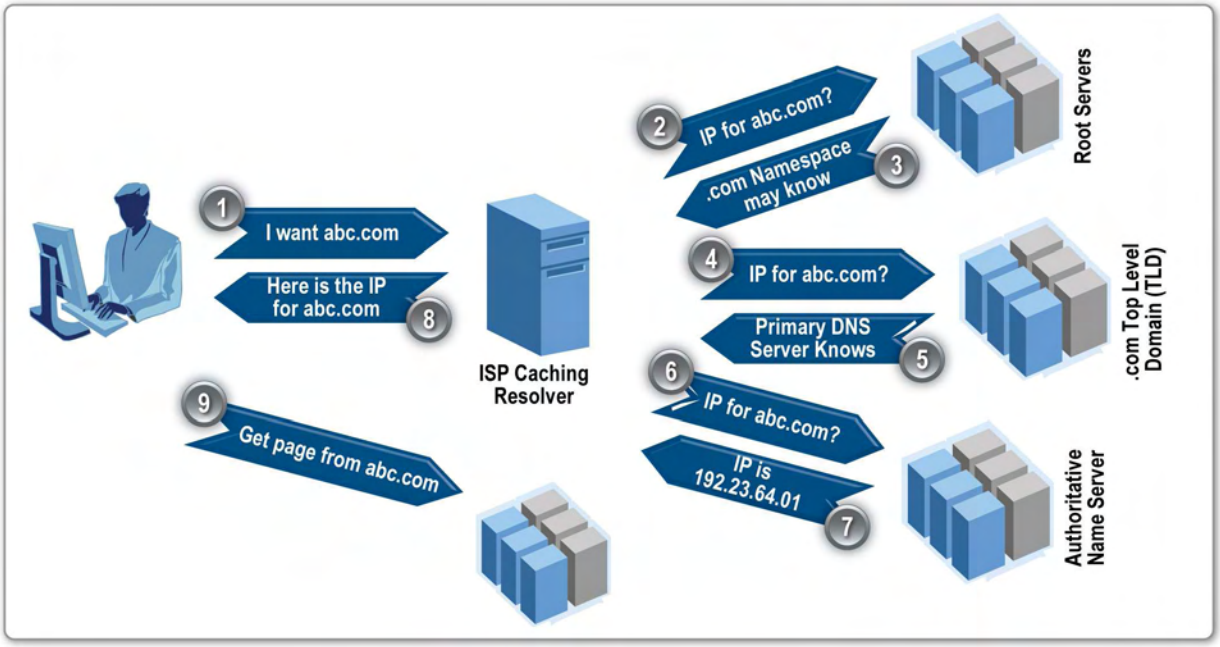


Figure 11: Sample DNS Query

The top level of the hierarchy is known as the root zone, or simply as "dot", which serves as an entry point to answer queries about the root zone and re-direct queries for zones lower in the hierarchy. Figure 11 illustrates the process for sample DNS query. Although there are currently 13 "root name servers" listed in the root zone, these point to hundreds of name servers worldwide that maintain DNS records for lower-level domains. Top-level domains (TLD) are delegated from the root to that TLD's name servers, such as .com, .org, .net, etc. (Figure 12) as well as to two-character country code TLDs (cc TLDs), such as ".us". Below the root zone, all other DNS servers are installed at different levels of the hierarchy and maintain only certain pieces of the overall DNS structure.

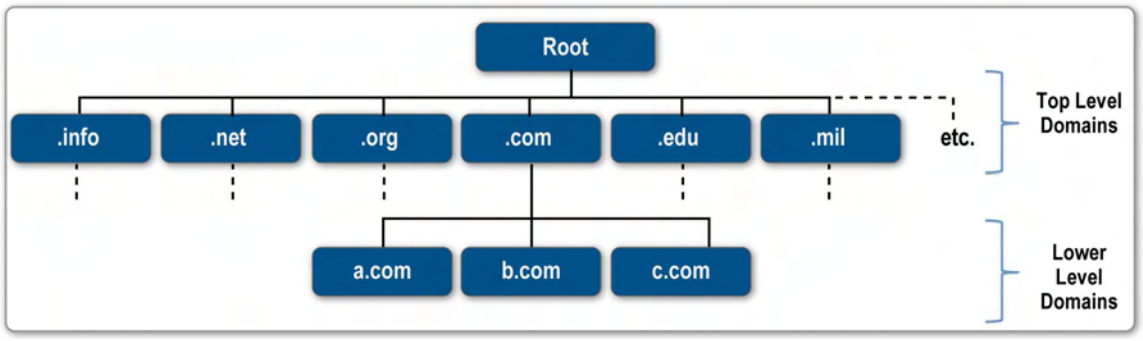


Figure 12: DNS Hierarchy

The IT Sector provides and operates domain registration services, TLD and root infrastructures, and resolution services that are essential to the operation of the Internet, as well as to the assurance of national and economic security and public health, safety, and confidence.[24]

The public and private sectors coordinate to provide five sub-functions in support of the *Provide Domain Name Resolution Services* critical function:

- Provide and Operate Domain Name Registry/Registrar Services;
- Provide and Operate Root, TLDs, and lower level Domain Services;
- Provide DNS Provisioning;
- Provide Name Resolution Services for Client Hosts; and
- Provide Security and Incident Management for DNS Operations.

3.2.1 Domain Name Resolution Services Attack Tree and Risk Profile

As detailed in Figure 13, SMEs assessed risk to the DNS function using an attack tree that focused on four undesired consequences that could cause adverse effects on the DNS infrastructure at the national level. Because of the wide range of vulnerabilities within the Provide Domain Name Resolution Services function, SMEs examined manmade deliberate, manmade unintentional, and natural threats to categorize possible methods by which a consequence could occur.

[24] Information Technology Sector Specific Plan (IT SSP), May, 2007.

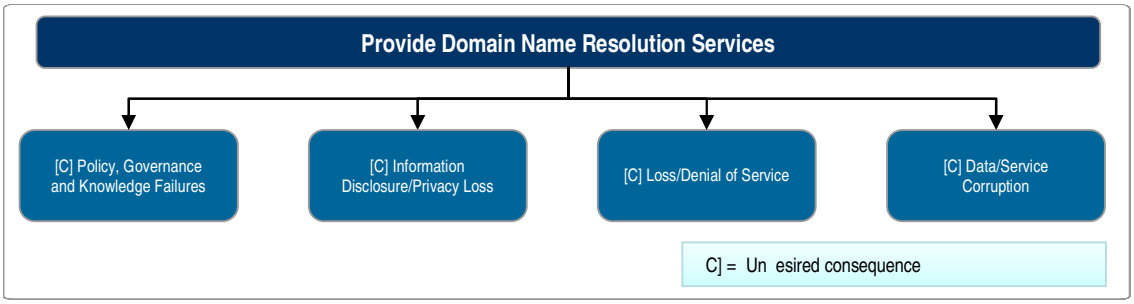


Figure 13: *Provide Domain Name Resolution Services* Attack Tree (Summary)

Policy, Governance, and Knowledge Failures

The Internet is an open and global system, providing individuals and organizations a variety of opportunities for attacking the DNS infrastructure. Actors attack the infrastructure for various motivations and objectives. An incident that originates from a nation-state may be motivated by a desire for political influence or to achieve military objectives. In contrast, an incident from an individual or a small group may only be a manifestation of their desire to exercise control over a key part of the Internet infrastructure or to demonstrate their technical prowess. Policy, governance, and knowledge failures could cause significant economic and national security impacts to the DNS critical function, and they could result in political and diplomatic tensions between the U.S. and nation-state threat actors.

Risk assessment SMEs identified four primary objectives for manmade deliberate threats to cause policy, governance, or knowledge failures to the DNS function:

- Politically-motivated attempts to influence or disrupt DNS operations;
- Desire for financial gain;
- Demonstration of technical superiority; and
- Gratuitous defacement or damage.

An attacker could try to establish an alternate Internet root, to which DNS inquiries could be diverted, instead of being directed to the "real" DNS root. The establishment of regional or alternative internets could decrease interoperability and cause technical confusion. Such a situation could cause strategic consequences across multiple sectors. Internet market influences may not be strong enough to avoid the emergence of an alternate, authoritative root, if the political and strategic environment provides an opportunity to establish and manage an alternative root system. Should an actor's political or strategic interests to establish and maintain an alternative root be economically advantageous, an actor's ability to exploit market forces and create an alternative root would be significantly improved. In addition, a competitor nation-state may desire to capitalize on the perceived control of the United States over the Internet by fragmenting the Internet, offering their own alternate root to undermine the perceived hegemony of the United States. Once Internet users become dependent on the alternate root, the actors would then gain political and economic leverage. Additionally, an alternate root that denied service for financial transactions could undermine the economic stability and security of the United States.

In addition to governance-related risks, knowledge failures, resulting from the lack of extensive quality assurance testing and DNS code and operational deployment review, can lead to significant vulnerabilities. Frequent changes to technology and inconsistent adoption of new standards could also pose vulnerabilities. Inconsistent or fragmented R&D, modeling, and simulation efforts could allow actors to exploit knowledge failures or false assumptions regarding the resiliency, redundancy, and capabilities of current and future Internet technologies, especially emerging technologies.

All members of the Internet community with R&D capabilities play an important role in the development of new protocols and other areas of innovation. An individual seeking to disrupt DNS operations would need the ability to promote production changes, potentially without employing sufficient quality assurance or production controls. Someone who has the ability and access to promote production changes could

unintentionally promote programming errors, quality assurance errors, or system administration errors. Disregarding standard testing procedures could result in an accident that could affect the operation of a DNS. Like most computer systems, system administrator actions for DNS services may be accessed remotely, so an unintentional threat would not necessarily originate with someone who is physically inside the facility where the DNS servers are located.

Top-level DNS services are potentially vulnerable to manmade attacks. Nation-states (including foreign military organizations), organizations, and individuals attack the root and the TLDs regularly.[25] A nation-state wishing to exercise its political will or military capabilities could launch an attack on the DNS country code servers that resolve domain names within a target country's country code domain, while simultaneously attacking other DNS and routing vulnerabilities. For example, if nation-state A were to launch an attack on the DNS servers for the ccTLD servers belonging to nation-state B, nation-state A may render Internet destinations in nation-state B's domain unreachable from other parts of the world.

Loss/Denial-of-Service

Loss/Denial-of-service can occur by a number of large scale attacks against the DNS infrastructure. Potential attacks could be either physical, logical/cyber, or a combination of both. Attacks may occur at any time since the DNS is continuously available. However, because DNS is a distributed system, an attack on one part of it would not necessarily paralyze the system. A DNS failure could be the direct result of both hardware and software vulnerabilities and may be impacted by manmade deliberate, manmade unintentional, and natural threats. DNS failure catalysts include strategic, political, and economic organizational and national agendas. Risk assessment SMEs identified three major concerns that could cause a loss or denial-of-service:

- Damage or attacks to the infrastructure supporting the DNS system, such as routing protocols, computer hardware, power supply lines, or phishing attacks;
- Lack of assessment and preparation for the simultaneous introduction of new technologies and protocols such as Internet Protocol version 6 (IPv6), Domain Name System Security Extension (DNSSEC), new gTLDs, and Internationalized Domain Names (IDN); and
- Poor or negligent software development practices, the lack of comprehensive code review, reckless or negligent deployment procedures, and the lack of fully understanding the ramifications of a particular configuration change.

Malicious actors on the Internet use mechanisms such as Distributed Denial of Service (DDoS) attacks, cache poisoning, traffic re-direction, and other exploits of the DNS and routing protocols. Additionally, organized crime syndicates have increased their ability to cause wide-scale financial fraud and harm on the Internet, but—to date—they lack the sophisticated resources that nation-states and other large organized cells might employ to conduct wide-scale coordinated attacks with cascading impacts. It has also been noted that organized crime syndicates rely on the Internet to conduct their operations. Therefore, a loss or disruption to Internet services would not be advantageous for the desired outcomes of these syndicates.[26] Cascading consequences could include denial or loss of service of electronic education and tracking systems, supply chain issues, disrupted or degraded electronic banking, shipment tracking, and Voice-over-Internet Protocol (VoIP) technologies, and credit trading. Loss of service could also be caused unintentionally by a construction crew that severs underground communications cables. Such an incident would have limited impact to DNS services if it occurred in isolation, but if the incident

[25] For a few examples of such attacks, please see the following: (1) Higgins, Kelly Jackson. "VeriSign Ups the DNS Ante: Tenfold capacity increase to DNS infrastructure, tighter security intended to blunt future DDOS attacks". DarkReading. Feb 8, 2007. http://www.darkreading.com/security/management/showArticle.jhtml?articleID=208804347; (2) ISC/UMD/Cogent. "Events of 21-Oct-2002". November 24, 2002. http://c.root-servers.org/october21.txt; and (3) Internet Corporation for Assigned Names and Numbers. "Root server attack on 6 February 2007". Factsheet. March 2007. http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf.

[26] Swartz, Jon. "Crooks slither into Net's shady nooks and crannies," USA Today: 10/20/2004 (http://www.usatoday.com/tech/news/2004-10-20-cyber-crime_x.htm).

involved multiple cable cuts, the availability of DNS and Internet services could be impacted over a wider area.[27]

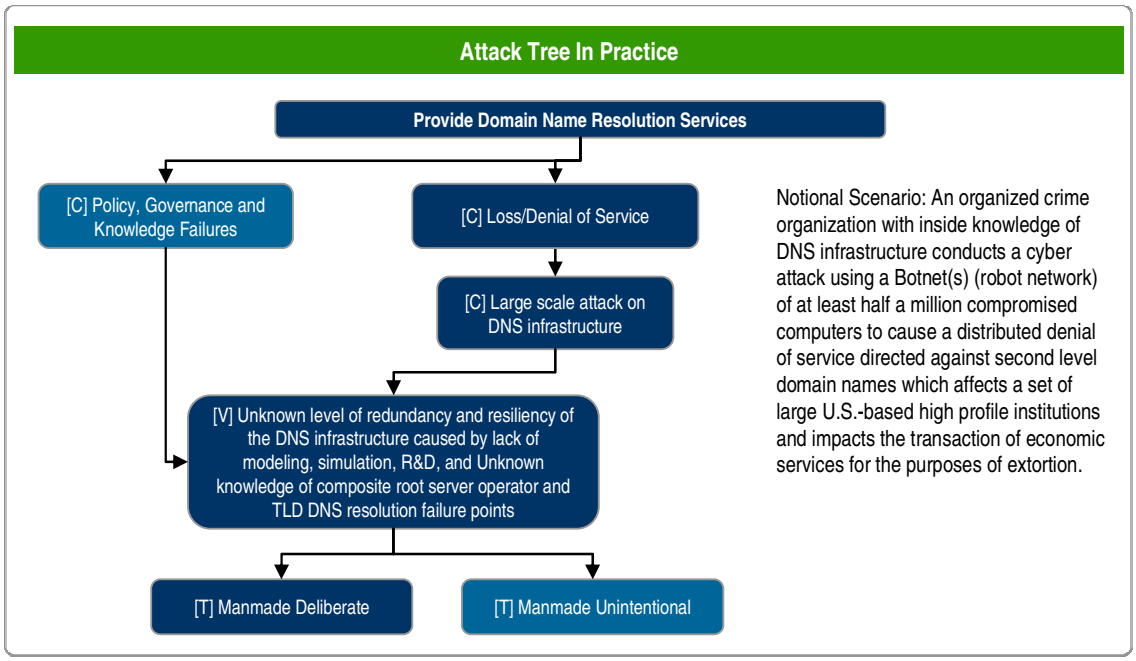


Figure 14: Notional scenario applied to the *Provide Domain Name Resolution Services* Attack Tree

In contrast to individual, group, or organized crime threats, nation-states have significant resources and capabilities to conduct simultaneous and attacks, including, but not limited to, destroying undersea and terrestrial cables; eliminating electricity access and degrading power grids; introducing counterfeit parts; physically disabling name servers at crucial chokepoints; large-scale DDoS attacks; and strategic cache poisoning. In addition, nation-states typically have more robust operational decision-making processes than an individual actor, group, or organization as well as more advanced capabilities to attack key areas of cyber infrastructure to cause potential consequences to national security. Nation-states also have the ability to attack the Internet at crucial points simultaneously which could compromise the DNS and the entire Internet on a global scale.

Most natural threats would only impact a single geographic region where there is a concentration of resources, limiting damage to that location. Aside from storms and earthquakes, most of the natural threats could be anticipated with varying degrees of warning and preparation. Producers and providers of this function would be aware of the threat before it actually occurs, so they could engage contingency and continuity plans, thereby mitigating the consequences of the natural event. In addition, natural threats are most likely to impact the infrastructure on which DNS relies. Section 3.5, *Provide Internet Routing, Access, and Connection Services*, describes these risks in greater detail.

The first-order consequence[28] of a manmade unintentional attack would most likely be a denial-of-service. An unintentional modification of a portion of the DNS infrastructure, such as loading an outdated zone file or incorrectly modifying DNS records, would cause the DNS to distribute pointers to the wrong addresses.

[27] For an example of such an incident, please see the *Los Angeles Times* article from February 1, 2008 by Michelle Quinn entitled "Undersea cable accident a test of the Internet" http://articles.latimes.com/2008/feb/01/business/fi-india1.

[28] First-order impacts directly affect the critical IT Sector function. Second-order impacts affect entities inside and outside the IT Sector that depend on the function or sub-function.

In this case, Internet destinations would be reachable only by the users who received replies from that DNS server. Shortcomings in modeling and simulation techniques could lead DNS operators to believe that a DNS hardware or software modification would operate reliably. However, under extraordinary usage levels, or if the DNS were to come under attack, the modification could prove inadequate to meet the threat.

Information Disclosure and Privacy Loss

An increasing number of nation-states have been seeking information regarding cyber warfare capabilities in order to prepare more effective attacks and increase their defenses. Protecting the confidentiality of information can reduce the length of an attack timeline and temper its overall consequences. Risk assessment SMEs identified two methods by which information could be disclosed: 1) recursive infrastructure and 2) cache disclosure. Many of the security compromises and breaches that have occurred in recent years have been related to vulnerabilities in the recursive or caching DNS server code. Four major concerns could lead to confidential information disclosure:

- Negligent use or mismanagement of cached data files, such as monitoring logs, disconnected and discarded hard drives, and USB memory keys;
- Poor or negligent software development practices;
- Phishing attacks; and
- Non-secure wireless networks (e.g., wireless, hotel or other guest type networks).

Because the operators of root DNS servers monitor the infrastructure continuously, they have easy access to logs and/or caches. They have the ability to send all or part of these to other personnel, as well as to transmit them around. This movement creates additional opportunities for unintentional information disclosure. When correct data protection procedures are not followed, or personnel are negligent, the actors can access log and/or cache information. Second order consequences, include tampering and/or spoofing and exploiting revealed vulnerabilities.

Broader quality control practices, comprehensive code reviews, and consistent deployment procedures, are needed to prevent negative impacts to the integrity of information. The lack of sufficient training to recognize malicious attempts to solicit information and/or identify social methods in which actors compromise security could impair the ability to perceive or thwart an attack.

Individuals or groups with political or financial motivations may attempt to attack TLD DNS servers to disrupt the operation of those servers. However, it is more likely that these individuals or groups would attack DNS servers of corporations or government agencies with the intention of disrupting a target's operations or stealing information. Attacks at the corporation- or government agency-level enable the actor to direct the attack at a specific target—rather than the broader infrastructure—to disrupt specific processes or steal specific information for personal or financial gain. Attacks on lower-level DNS services are frequently attempts to copy the records in the DNS zone. A "zone transfer" gives the attacker a copy of the DNS records, indicating the addresses, aliases, and identities of objects in the DNS. This information can be exploited by an attacker, whose real objective is compromising or stealing Internet content.

Data and Service Corruption

Risk assessment SMEs noted a particular concern with defending the integrity of the DNS function against cyber crime and deliberate nation-state attacks designed to cause service corruption. The three areas of concern for data/service corruption are:

- Protocol vector[29] through facilitated man-in-the-middle (MITM)[30] attacks, as well as data injection through hacked user accounts and/or social engineering attacks;
- System compromise through MITM attacks or disgruntled/coerced personnel; and
- Repository corruption by obtaining registrar information from a WHOIS[31] service.

An individual with system administrator or "superuser" access privileges to a DNS server could pose the highest threat to the system. A single high-access employee could write and deploy malicious configuration changes and could be coerced into making these changes, even if he or she had no intention of causing damage/corruption. Exploiting the DNS function would be difficult without the cooperation of a high-access employee. With the cooperation of an employee, the attack could be as simple as shutting down specific network hardware or software components.

Figure 15 summarizes the relative risk to the *Provide Domain Name Resolution Services* function. As noted throughout the *Provide Domain Name Resolution Services* discussion, in general, a nationally significant attack against the DNS function would most likely be part of an attack against another element of the IT Sector infrastructure, which caused collateral damage to the DNS. The availability of the function is of concern to the IT Sector in the context of the breakdown of the current single, interoperable, and global Internet, as well as large scale attacks to the DNS infrastructure. Also, of concern are impacts to the integrity and confidentiality of the function that could be caused by data or service corruptions resulting from accidents. Mitigation strategies addressing the policy-related risks highlighted below should be addressed collaboratively by public and private sector partners.

[29] A protocol is the format and procedure that governs the transmitting and receiving of data. A protocol vector may include the packet structure of the data transmitted or the control commands that manage the session, or both.
[30] Also known as a replay attack, a MITM attack occurs when transmitted information is intercepted covertly without authorization, altered, then retransmitted to trick a receiver into unauthorized operations, such as false identification, authentication, or a duplicate transaction.
[31] WHOIS is an online public database updated by a registrar that is a master directory for domain names.

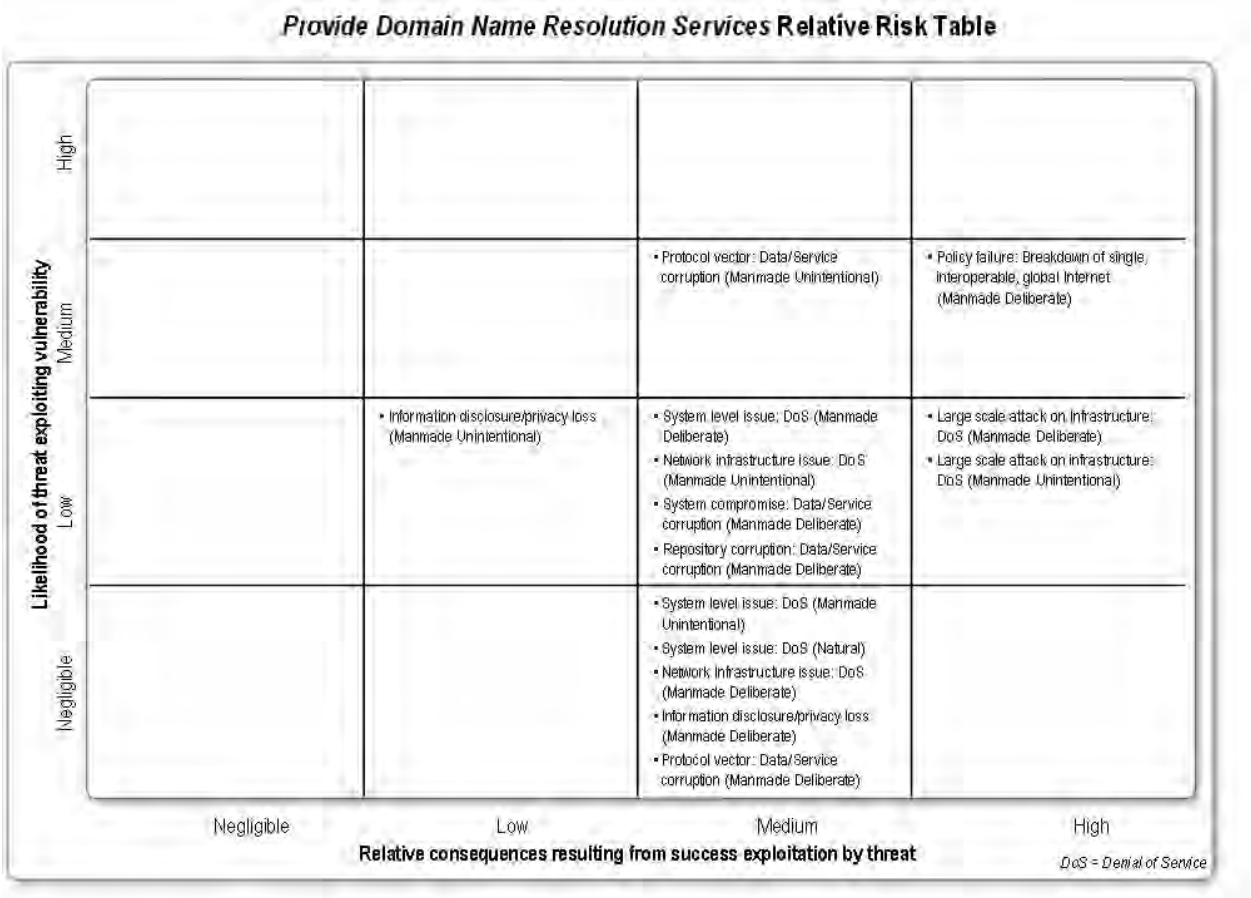


Figure 15: Relative Risks to the *Provide Domain Name Resolution Services* Function

3.2.2 Mitigations

As part of the Baseline Risk Assessment, the SMEs identified existing and future mitigations that address the risks outlined for the *Provide Domain Name Resolution Services* function. The mitigations were categorized as existing mitigations, mitigations currently being enhanced and improved, and future mitigations. These categories will assist the IT Sector outline R&D and protective program priorities.

Existing Mitigations

- Processes that enhance quality assurance and ensure continuous monitoring: Current mitigation strategies to prevent the breakdown of key network components within the DNS infrastructure include the continuous real-time monitoring of production equipment by network operations centers to anticipate and protect DNS infrastructure from malware attacks. Mitigations currently in place for preventing malicious configuration changes by a high access employee include process checks to avoid deployment of detrimental code and requiring multiple authentications for the deployment of production code.

- Infrastructure diversity: The DNS servers that maintain the DNS root and many of the TLDs are distributed around the globe. Because DNS is a distributed system, an attack on one part of it would not necessarily paralyze the system.

- Provisioning and the use of Anycast[32]: The root and top level domain operators continuously monitor the bandwidth used by the DNS during normal operations, as well as when under attack. Bandwidth is provisioned accordingly to be able to handle several orders of magnitude in increased traffic levels, such as during massive DDoS attacks. Additionally, the use of Anycast allows operators to supplement the DNS server infrastructure with more systems "behind the scenes" and to allocate additional resources quickly to specific areas under attack.

Mitigations Currently Being Enhanced and Improved

- Infrastructure diversity: The DNS infrastructure is distributed around the globe, which gives it an inherent resiliency. However, exploitation of a software vulnerability in the DNS Berkeley Internet Name Domain (BIND) code could be exploited simultaneously in a number of DNS servers. Much of the root and top level domain infrastructure does not depend solely on BIND, but a large portion of lower level domains and resolvers are dependent on BIND. Because they are well-known Internet resources, the top-level DNS servers are frequently targets of DoS attacks that flood specific TLD DNS servers with DNS resolution requests. The IT Sector is investigating enhanced methods, techniques, and means for TLD server operators to monitor incoming and outgoing traffic to detect attacks and to protect their systems from vulnerabilities.

- Implementation of DNSSEC: There is an extension to the DNS protocol to authenticate and enhance the integrity of DNS queries. DNS operators are considering implementing DNSSEC as a means to combat MITM attacks.

  When an end-user queries the DNS (or their ISP performs the query on their behalf), the current form of the DNS uses the first answer received from a name server, regardless of the answer's origin. MITM attacks exploit this vulnerability by returning an answer before the true authoritative server's response is received by the user, injecting the data that actor desires. The end user's system implicitly trusts this data, causing legitimate domain names to resolve to incorrect, bogus, or criminal systems. From there, well disguised phishing sites may be used to steal identities or to gain access to financial data.

  DNSSEC mitigates the risk of MITM attacks by adding digital signatures to query responses. When an end user queries a DNSSEC-signed zone, the name server returns not only the response, but also a set of signatures. Therefore, the end user's systems have the ability to cryptographically validate the signatures. If the signatures are determined to be invalid, the end user's application may throw the result away, or warn the user that the signature did not validate.

  For DNSSEC to be deployed successfully and its benefits fully realized, components need to be installed and signed in the root and all TLD zones. Also, DNSSEC must be installed at each second level zone, all ISPs, corporations, and institutions that run caching resolvers, end user operating systems, and any application utilizing the DNS. This is needed to ensure that the "chain of trust" is complete from the start of a DNS query, through all name servers and caching resolvers, and back to the end user. DNSSEC deployment is in the early phases of implementation and will take many years and strong public and private support to complete.

[32] The next generation IPv6 protocol utilizes three types of routing schemes: unicast, multicast, and anycast. Unicast is basic one-to-one communication, whereas multicast is one-to-many communication. A new type of routing scheme, called anycast, routes data to the nearest or best destination router within a group and can send a message to any single machine that was intended to receive it. This is similar to a multicast since any machine on a list can receive a message, but only the recipient with the most efficient route is chosen. Anycast is typically used as a way to provide high availability and load balancing for DNS, since the function is distributed over multiple geographically dispersed servers. (Sources: 1) Warnock, Mathew. "IPv6: The Next Generation Internet Protocol" IAnewsletter. Vol. 7, No. 3. Winter 2004/2005. http://iac.dtic.mil/iatac. 2) Internet Corporation for Assigned Names and Numbers. "Root server attack on 6 February 2007". Factsheet. March 2007. http://www.icann.org/announcements/factsheet-dns-attack-08mar07.pdf

Potential Future Mitigations

- Enhancing national-level modeling and simulation capabilities: A primary cause of manmade unintentional threats is a lack of training and careless operation. The implementation of new technologies and protocols, such as IPv6, DNSSEC, new gTLDs, and internationalized domain names, could pose potential risks, making administrative training absolutely critical to security. National-level and multi-discipline modeling and simulation efforts could assist in the development of a more unified effort to mitigate accidental risks. This could encourage investment into new technologies to expand beyond the DNS, as well as trigger the need for effective training. Prioritizing and budgeting for mitigation techniques, such as full system modeling research and robust code deployment policies to address knowledge failures regarding the resiliency, redundancy, and capabilities of current and future Internet technologies is needed. Extensive code review, exhaustive quality assurance of production code, and load testing of any approved changes prior to going live can further mitigate risk. A possible mitigation strategy to deliberately injecting or unintentionally activating erroneous or malicious code at any time is to limit product code deployment to certain hours of the day.

- Conducting exercises to test DNS services: The development and practice of operational exercises is needed to address technical vulnerabilities within the DNS in the event that a physical or logical attack degrades or disrupts any of number of DNS servers. The DNS server corruption threshold that would render domain name translation incapacitated is not well known. An increase in full system modeling and simulation efforts to help identify possible courses of action in the event of an emergency and to predict possible outcomes can further help mitigate risk. Additionally, these efforts should look to mitigate the current knowledge gaps regarding DNS vulnerability threshold levels and the security and stability impacts of the simultaneous introduction of new gTLDs, IDNs, DNSSEC, and IPv6.

- Enhance the security of DNS servers: To improve DNS security and stability, the IT Sector may want to undertake efforts to improve the structural integrity of DNS servers. Additionally, improved physical and logical security of DNS servers will assist in guarding against potential attacks, both manmade and natural.

3.3. Provide Identity Management and Associated Trust Support Services

Provide Identity Management and Associated Trust Support Services Function Summary	
Situation	The IT Sector uses identity verification to authorize access to Internet content and conduct operations that support elements of each of the critical IT Sector functions. The IT Sector also provides identity management services to content providers. Identity management products, such as identity credentials, user names, and passwords, help manage online identities and secure data.
Concern	The most significant security gap in online identity management is ensuring that the person claiming an identity is actually the person to whom that identity belongs. Some identity management technologies, such as PKI, offer a high level of identity assurance. Biometric identifiers offer higher levels of assurance, but biometric identification technologies are not mature enough to be widely deployed, and these may raise privacy concerns.
Impact	The security of physical identity credentials, such as drivers' licenses and passports, has been improved with new materials and production techniques that make them more resistant to forging and alteration. Online electronic identity credentials, such as usernames and passwords and PKI certificates, offer tradeoffs in convenience, cost, and complexity.

Identity management systems are used to issue identity documents and credentials under the authority of a government agency or a company. For example, an identity document might be an employee or student identification (ID) card, a driver's license, a passport, or a Social Security card. Credit cards, retail loyalty program cards, or military ID cards grant access to specialized types of transactions or privileges. This identity management concept also applies to online systems. The simplest example is the use of username and password combinations to obtain access to computer networks, financial accounts, e-mail systems, and other types of online services.

One of the most common methods for establishing trust in a user's identity is the use of identity credentials that are issued only after verifying the individual's identity. The identity credential is usually only the physical manifestation of a comprehensive identity management system that may administer the entire lifecycle of identity credentials. Though some identity management systems have more or fewer steps, the general components of an identity management system are:

- *Design identity system:* Establish the objectives for the identity management system, determine security and assurance level requirements, and design and build systems and infrastructure to carry out those objectives.

- *Authenticate applicants:* Develop systems and procedures to verify the identity of individuals and the authenticity of documentation and other identifying information that will be accepted to verify that identity.
- *Issue credential:* Create and issue the credential, and deliver it securely to the subject.
- *Manage credential:* Oversee the use of the credential, renew or re-issue credentials periodically, audit the operation of the identity management system, and adjust the security and operational procedures of it if requirements change.
- *Revoke credential:* Revoke, suspend, or recover the credential when it is no longer needed, and develop procedures for archiving credential records.

Similar to the other critical functions, identity management systems are subject to threats to their operation, use, and integrity. Some identity credentials, such as a driver's license, may be accepted if they look legitimate. Others, like a credit card or an identity document that has an electronic element or that may require online authorization, may only be accepted if they act legitimately. Identity management systems are responsible for determining the legitimacy and authenticity of identity credentials, such as establishing a strong level of trust in the identity of a user. The managers of those systems are responsible for analyzing threats to those systems and mitigating the risks those threats present.

This section analyzes the risks and risk mitigation steps that apply to the entire spectrum of identity management systems. For the most secure forms of identity credentials, such as digital certificates, the Certificate Authority (CA) is the foundation of the identity management system. However, other, less secure forms of identity systems are used in the IT Sector, such as username and password, as well as physical identity tokens.

A CA is a trusted organization responsible for establishing the identity of the user to a very high level of certainty, and then issuing PKI digital certificates in an identity credential. To support digital certificate services, the IT Sector provides and operates CA registration and validation services that are essential or critical to the assurance of national and economic security and public health, safety, and confidence.[33] Public and private sectors coordinate to provide six sub-functions in support of the *Provide Identity Management and Associated Trust Support Services* function and the overall phases of a PKI identity management system:

- Provide organizational digital identity and certificate provisioning services;
- Provide individual digital identity and certificate provisioning services;
- Provide organizational revocation services for digital identity and certificate;
- Provide individual revocation services for digital identity and certificate;
- Operate infrastructure for trusted root certificate authorities; and
- Ensure the chain of trust and the ability to attest to it.

National-level CA responsibilities include:

- *Registration Authorities (RAs)*, which act as local agents for a CA to register and verify the identity of users to whom PKI certificates will be issued. RAs are responsible for verifying user requests for digital certificates, and for asking the CA to issue them. RAs request digital certificates that enable companies, other organizations, and users to exchange information and money safely and securely.[34]
- *Certificate Authorities*, which are responsible for issuing and managing security credentials and public keys for identity, message encryption, and other purposes. CAs check with a Registration Authority to verify the information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can issue a certificate.[35]

[33] Information Technology Sector Specific Plan (IT SSP), May 2007
[34] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214245,00.html
[35] http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213831,00.html

- *Root Certificate Authorities*, which are responsible for issuing and managing security credentials for other CAs. A Root CA is the "trust anchor" for the "chain of trust" in a PKI system.

3.3.1 Identity Management Attack Tree and Risk Considerations

The *Provide Identity Management and Associated Trust Support Services* attack tree (Figure 16) highlights three primary undesired consequences that could cause adverse effects on the Nation's critical infrastructure. Under these undesired consequences are various vulnerabilities that could adversely affect the IT Sector's ability to provide identity management services to its consumers.

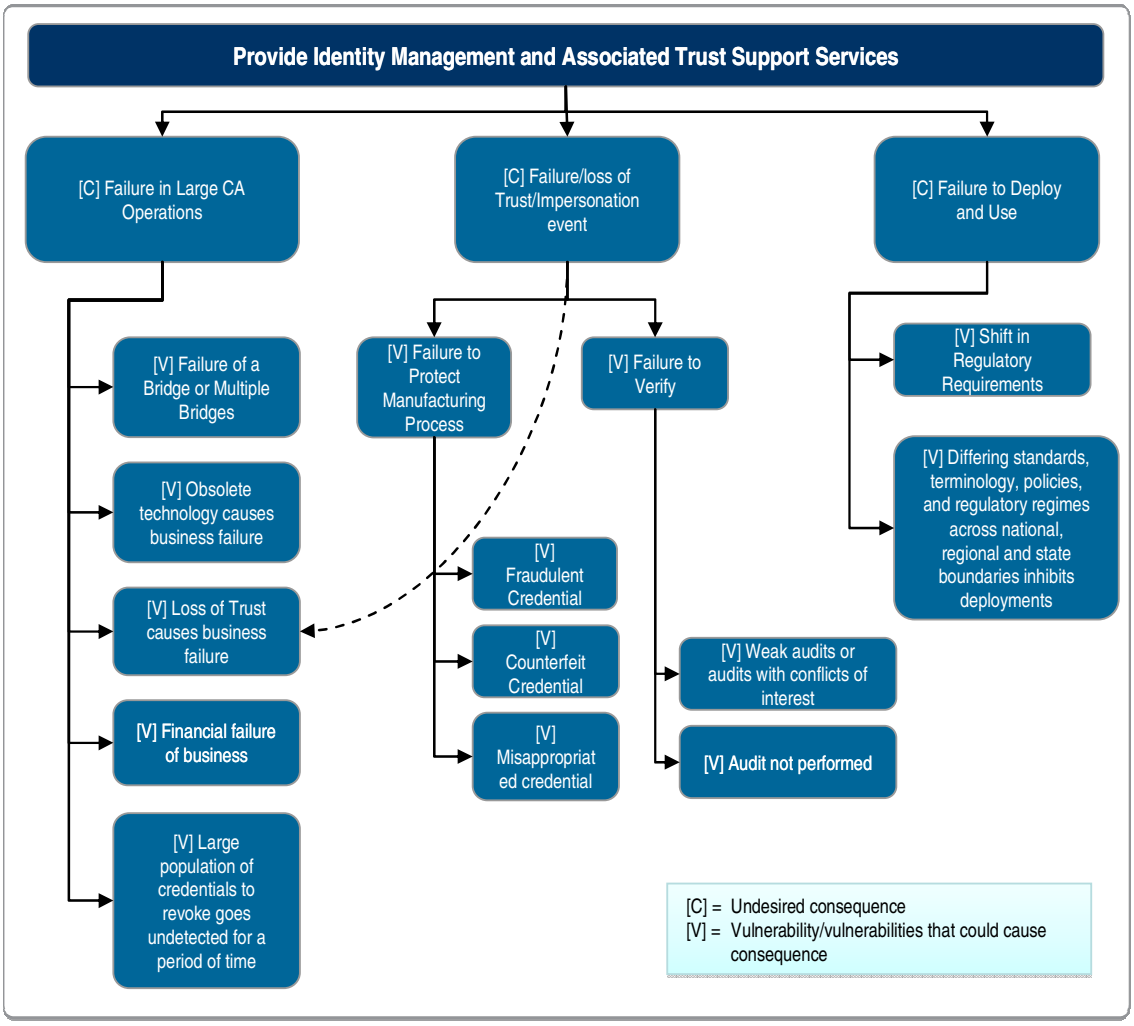


Figure 16: *Provide Identity Management and Associated Trust Support Services* Function Attack Tree

Although digital certificates have been recognized as secure and reliable identity credentialing tools available today, they impose costly and complex administrative burdens on organizations that use PKI) certificates. Until these issues are resolved, the high level of assurance that digital certificates provide may remain the exclusive province of organizations that have the resources to support them or that require the levels of assurance and non-repudiation that PKI can provide.

The President's National Security Telecommunications Advisory Committee (NSTAC) Identity Issues Task Force (IdITF) is examining the issue of identity management. A comprehensive approach to identity

management is needed to improve assurance that the person requesting electronic access is indeed, that person. As reviews and analyses like that of the IdITF are completed, risk assessment SMEs intend to leverage their outputs and findings to conduct additional risk analysis of the *Provide Identity Management and Associated Trust Support Services* function.

Due to the need to address the security of original identity documents, the content associated with this function only highlights *potential* risks to the function. Relative ratings or analyses have not been provided. Instead, public and private IT Sector partners identified this as an area that requires additional study before determining the overall risk to the function.

Failure in Large CA Operations

The failure or corruption of a large CA, in particular a Root CA, would have negative impacts throughout the IT Sector. A root CA is responsible for verifying and validating the identity of lower-level CAs. This hierarchical trust model ensures that a rogue CA cannot function unchecked. The failure of a root CA would trickle down to lower level certificate authorities and ultimately impact an Internet user's ability to verify the identity of a Web site.

The failure of a CA or a root CA could be caused by any number of factors including:

- Obsolete technology;
- Loss of trust;
- Financial failure of business; and
- Large population of credentials that are not revoked in a timely manner.

In theory, a CA could fail if the organization that ran it neglected to update, secure, or maintain its infrastructure. For example, security researchers have recently demonstrated flaws in the Message-Digest algorithm 5 (MD5)[36] hashing algorithm that could be exploited to create different PKI certificates that have identical checksums.

A malicious actor could exploit this vulnerability to forge a certificate and use the forged certificate to impersonate a trusted Web site, such as an online bank or an e-Commerce storefront. This type of attack would be very difficult to detect because the forged certificate would appear, even to a knowledgeable Internet user, to have been created by a trusted entity.

If this type of forgery attack took place, Internet users may lose confidence in the CA infrastructure. As a result of this loss of confidence, it is possible that one or more large CA could go out of business if consumers sought CAs with more secure technologies, processes, and procedures. The failure of one large CA, particularly a root CA that had issued thousands or millions of certificates would have widespread impact across the cyber infrastructure.

Failure/Loss of Trust/Impersonation Event

Most identity management systems issue some type of identity credentials to individuals whose identity has been verified during the credential creation and issuance phases of an identity management system. A credential may be a simple means to verify the identity of the individual, who may be referred to as the *subject*, such as a username and password. For applications that require a greater degree of certainty, the credential may be a physical document or token, such as an identification badge, a driver's license, or a passport. It may also have biometric identifiers, such as the subject's photograph or fingerprints.

[36] MD5 is a "one-way" 128-bit hash function developed by RSA (http://www.rsa.com/rsalabs/node.asp?id=2253). A hash function is a cryptographic algorithm that generates a fixed string of numbers from a text message. The "one-way" means that it is extremely difficult to turn the fixed string back into the text message. "One-way" hash functions are used for creating digital signatures for message authentication.

A physical credential that incorporates electronic identity elements affords an even greater level of assurance that the credential bearer is indeed the subject to whom it was issued. A U.S. government-issued Personal Identity Verification (PIV) card or a Department of Defense Common Access Card (CAC) has PKI digital certificates stored on the card. The PKI certificates on a PIV card or a CAC are only issued after a subject is approved following a rigorous third-party examination of his or her identity documents.

The CAC and PIV have three digital certificates, which are used to identify the subject, to digitally sign documents and e-mail messages and encrypt files and messages. The CAC and PIV also have a digital copy of the subject's photograph and digital representations of the subject's fingerprints stored on the card and other biometric and personal data.

In the past decade, identity credentials have become more widely used and more frequently required in order to conduct everyday activities. Identity credentials are used to control and prevent crime and terrorism, as well as to conduct ordinary activities, such as controlling building access, obtaining a job, opening financial accounts, and flying on airlines. Identity credentials are increasingly needed for every day use. Those who acquire or use them for criminal or unlawful purposes pose threats to the integrity of identity systems, as well as to society at large.

The impact to the identity management service producers' and providers' sustained ability to deal with loss of trust or impersonation events could cause significant and lasting economic and national security consequences. The following four situations illustrate this type of impact:

- First, one of the simplest ways to obtain a genuine identity credential is to get one at the point of manufacture, where legitimate credentials are issued. Employees who work with the physical credential media or those who have access to the systems that authorize and create credentials are often the source of genuine, if improperly issued, identity credentials. These credentials are the most dangerous ones, because they not only look and feel like genuine credentials, they in fact are genuine albeit fraudulent and counterfeit credentials.

- Second, fraudulent credentials are frequently inadvertently issued because the documents used by a subject to get the credential are themselves fraudulent. A Social Security number is required to qualify for employment in the U.S., but employers frequently fail to determine if the subject's Social Security card is genuine or if the Social Security number actually belongs to the subject. Fraudulent drivers' licenses, frequently issued by States that do not have or have not had rigorous identity or application verification systems, remain a persistent problem. More rigorous identity verification procedures are intended to reduce the incidents of fraudulent drivers' license credentials.

- Third, detecting counterfeit credentials requires thorough inspection. Although materials and more sophisticated manufacturing techniques have made credential counterfeiting a more difficult and more technically challenging process, counterfeit detection still poses a problem. The responsibility for detecting a counterfeit credential frequently falls to a credential inspector, who may only casually inspect the credential, who may not know what a real version of the credential looks like, or who may not inspect it at all. One of the significant benefits of electronic credential elements, such as digital certificates, is that the logical elements of an electronic credential can be extremely difficult to counterfeit. The bearer of the credential may not have the means to verify that those elements are correct, or that they even exist. The added cost and complexity of electronic credential elements raise the bar against counterfeiters, though they do not eliminate the threats of counterfeit credentials.

- Fourth, a lost or stolen credential can be particularly dangerous since it is both genuine and it has been properly issued to an authorized subject. Even if the credential has a photograph on it, a cursory inspection of the credential may not indicate that it does not belong to the person who has the credential. The electronic elements in a misappropriated credential usually require a PIN

or a keyword to use them, and the holder of a stolen credential would not necessarily know that access code.

A second branch of the Failure/Loss of Trust/Impersonation Event part of the Identity Management Attack Tree addresses the Failure to Verify. This branch includes verifying credentials as well as auditing identity credential systems. Like a financial system, an identity management system should be audited periodically to determine if it is operating correctly and if it is being maintained properly. Audits may be performed by the credential issuing organization, or by an independent, third-party auditor. Some parts of the identity management system may not be controlled by the credential issuer, such as the CA for PKI certificates. However, the identity management system should be audited to identify inactive, expired, or dead accounts, revoked or expired credentials, and to improve system efficiency and security.

The most challenging aspects of auditing an identity management system are identifying inactive or expired accounts and credentials and enacting procedures to recover, revoke, or destroy those credentials. Deactivating an account, such as by deleting a username and password from an access control list, is relatively simple, but recovering a lost, stolen, or revoked physical credential is not. Determining the accounts that should be deactivated may not be simple, although the system may be able to determine which accounts have been inactive for a period of time. It may not be possible to recover a lost or stolen credential, but the credential identifier may be put on an invalid credential list, or the digital certificates revoked, to reduce the risk of the credential being used. In any case, credentials must be verified at the time of use in order to reduce the risk of unauthorized use.

A weak audit may give those responsible for the identity management system a false and misleading sense of security. A weak or cursory audit may only examine the system records and documentation. This type of audit would establish only that there are procedures that should be followed, and that records have been maintained about which credentials have been issued. A more thorough audit would examine how the identity verification, identity document validation, and credential issuing steps are actually being performed. It would also evaluate the adequacy of the procedures and compare the system documentation, identity validation, document validation, and credential issuing procedures to those used in other systems. A comprehensive audit would sample the set of issued credentials and subject accounts to determine the extent of dead, invalid, or inactive accounts. It would also determine the adequacy of procedures to revoke credentials, and to notify relying parties about revoked or invalid credentials.

Audits should be conducted by an impartial third party that can evaluate identity management system procedures and processes objectively. Moreover, a third party auditor can compare the procedures and processes to those used in other identity management systems and develop or recommend best practices for running an identity management system.

Some IT organizations audit their identity management systems infrequently, or only do so when they perceive a threat to the integrity of the system. They may not see the benefit in auditing an identity management system, or they do not think it is worth the effort. An identity management system that is not audited or that is lightly audited presents an opportunity and a target for people who may benefit from its misuse.

The threat to identity management systems are real, and despite improvements and advances in identity credentials, personnel training, and security, no identity management systems are risk-free. Credential technology has made it more difficult to forge, alter, or duplicate legitimate credentials, and electronic elements, such as digital certificates, increase the level of assurance of credentials. However, human factors in the design, control, and management of identity management systems remain the greatest risks.

Most threats to identity management systems are from deliberate actions that are conducted by individuals or organizations that can benefit from the unauthorized or unlawful access to buildings, systems, and information. Depending on the target and severity of the attack, a threat can go undetected for a long duration, thereby making the target susceptible to exploitation. Stolen, counterfeit, forged, or

fraudulent identity credentials can be used for some time, until some act or action reveals the presence of an interloper or an intruder.

Deliberate identity management threats can pose a longer-lasting danger than threats that can be detected relatively quickly. A physical intrusion attempt, for example, can be detected immediately if an alarm sounds when the break-in is attempted. However, an intruder with a valid, misappropriated electronic identity credential that provides system administrator privileges can examine system functions to uncover system weaknesses and vulnerabilities that can be exploited effectively at a later time.

The motivations for deliberate threats to identity management systems vary, but they range from relatively low-threat recreational hacking to higher-level threats, such as identity theft, crime, and terrorism. Fraudulent or forged credentials are frequently used for a range of actions, starting with underage drinking, and moving up the threat chain to driving with a suspended or revoked license, qualifying for employment, and gaining entry to buildings and countries under false pretenses. Compromised physical and electronic identity management systems can give individuals or organizations unauthorized access to both environments if security is not coordinated between them.

Unintentional threats to identity management systems are those that may be made by neglect or by ignoring standard security procedures. Neglect may include a variety of issues, such as not signing off a system properly when leaving a computer terminal; leaving identity credentials unattended or unsecured; or writing down a Personal Identification Number (PIN) or password and storing it in the open or with the credential. These examples illustrate the threat of ignoring documented security procedures, while losing a credential is an unintentional threat and can occur for a variety reasons, including recklessness or carelessness.

Identity management systems are usually not affected by natural threats. However, a natural catastrophe, such as a storm, flood, or fire, could affect the operation of the computer systems run by a CA. Natural threats could also interfere with the operation of systems that check or validate credentials used for physical or system access.

Failure to Deploy and Use

A comprehensive identity management system employs a full system lifecycle, including establishing an identity issuing authority to verifying identities, issuing credentials, and revoking and terminating credentials. Some agencies and organizations implement only enough of an identity management system to give its employees or constituents system or building access or to grant privileges. These partial implementations may work for the limited purposes for which they are intended. Motorists can drive legally, employees can get into a building to work, and users can log into computer systems to access their accounts.

However, the minor flaws of these partial implementations can be exacerbated during times of crisis, such as security problems, stolen, forged, or counterfeit credential use, unauthorized system access and hacking, crime and safety problems in workplaces, and identity theft. There are many reasons for failing to deploy and use a comprehensive identity management system, and many organizations have seen the consequences of such a short-sighted approach.

The regulatory and legal environment frequently affects the implementation of identity management systems. Recent improvement in the quality of identity credentials and in identity management systems has been in response to real and perceived threats of terrorism and crime. Employers now must bear more responsibility for protecting their employees, as well as determining if they may be legally employed. At the same time, privacy laws have raised standards for collecting, storing, and maintaining the personal information on which identity decisions are based. Government agencies and commercial firms must balance the often conflicting demands of determining an individual's identity with protecting that information from exposure, even when it might be used to verify the individual's identity.

Federal and State agencies and commercial companies have different responsibilities for issuing and maintaining identity credentials. These responsibilities are rooted in the defined powers of Federal and State agencies, and the private interests of corporations. The Federal government, for example, issues passports, while the States issue driver licenses, and companies issue identity badges to their employees. Under appropriate circumstances, Federal and State agencies and companies may share the identity data they have with law enforcement and tax agencies. However, the differing types of authority the three entities have inhibit the development of a single, coordinated identity management system.

3.3.2 Mitigations

As part of the Baseline Risk Assessment, the SMEs identified existing and future mitigations that address the risks outlined for the *Provide Identity Management* function. The mitigations were categorized as existing mitigations, mitigations currently being enhanced and improved, and future mitigations. These categories will assist the IT Sector outline R&D and protective program priorities.

Existing Mitigations

- Process controls: Identity management functions mitigate manmade threats by carefully controlling the credential creation and issuing process, developing rigorous identity verification processes, enhancing physical credentials with features that make credentials more difficult to copy or alter, embedding electronic identity elements, such as PKI certificates, incorporating biometric identifiers, such as photographs and fingerprints, and requiring identity checks in everyday activities. Many systems subject passwords to complexity rules that govern the length and character mix of passwords, as well as require frequent changes of passwords.

- Technology solutions: Digital certificates and other electronic identity verification systems have been deployed in cases where government agencies and businesses have deemed the cost and complexity of those technologies to be worthwhile. Even though the benefits of digital identity technologies have been proven, many government agencies and businesses have chosen to use simpler technologies that can be embedded in a physical credential. Making common identity documents, such as passports and driver licenses, more difficult to forge or alter is less expensive than incorporating PKI certificates in these documents.

  Forged, altered, or counterfeit identity credentials are a significant problem, despite the implementation of steps to make the most desirable identity credentials difficult to duplicate or forge. In recent years, credential-issuing agencies have employed a number of high-tech measures to make identity credentials resistant to forging and tampering. Laser printing and engraving, sealed plastic lamination, patterned overlays, ghost images, optically-variable devices, microprinting, ultraviolet overprinting, and other techniques have made high-quality identity credentials more difficult to reproduce or to alter.

- Audits: Many identity management systems are audited periodically to determine if they are operating correctly and if they are being maintained properly. In addition to internal audits, audits should be conducted by impartial third parties evaluate identity management system procedures and processes objectively. Third party auditors also compare procedures and processes across other identity management systems to develop or recommend operational best practices. These best practices include standards for audits that are similar to.

Mitigations Currently Being Enhanced and Improved

- Improved technology solutions: As more attention is paid to data protection and the identity credential lifecycle, enhancements/improvements are being made to identity management. As physical credentials expire or a new generation of physical credentials is introduced, new technologies and physical and electronic elements are deployed in the credential to make it

harder to duplicate, alter, or forge. These elements are constantly being improved, even though they have not been incorporated into older versions of the credential that are still valid.

- Electronic identity elements: Although the value of electronic identity elements, such as digital certificates is clear, a number of technical, administrative, and cost issues prevent them from being implemented. Currently, only the most secure identity management systems implement all of these elements. Digital certificates impose heavy administrative and cost burdens on their issuers; the certificates expire, and PKI systems tend not to scale well. However, many organizations have concluded that, despite challenges, digital certificates are the most secure and most practical authenticators available today. Military and government agencies are deploying new, high-assurance identity management systems to raise identity assurance.

- Multi-factor authentication: Multi-factor authentication is a process by which the user provides two or more independent means of identification: "something you know," "something you have," and/or "something you are." The "something you know" is typically a username and password in combination or things commonly known only to the user, such as images or words. The "something you have" is typically a physical credential or device, such as a smart card, a hard token, or an identity credential. The "something you are" is typically a biometric identifier like a voiceprint, fingerprint, or signature. Access to the target system is controlled through multiple means, thereby mitigating the risk and raising the level of assurance of the identity of the individual seeking access. This mitigation is currently found in high security organizations, but it is gaining popularity in others as well.

- Improved system audits: Auditing IT systems is a relatively new practice, but its use has grown as corporations, government agencies, and other organizations have become dependent on the operation of data processing and other IT systems. IT auditors have developed their own auditing standards that are similar to the auditing standards used to audit an organization's financial records. Identity management system auditing has not reached the same level of maturity as financial auditing. However, IT system auditors are developing standards for identity management system audits, as well as policies that govern those standards.

3.4. Provide Internet-based Content, Information, and Communications Services

Provide Internet-based Content, Information, and Communications Services Function Summary	
Situation	Consequences resulting from unintentional threats to the function can often be traced to the DNS or Internet Routing functions. Unintended Border Gateway Protocol (BGP) changes or improperly updated BGP tables can cause impacts to the availability of Internet content. Also, there are instances when disruptions in the DNS function can cascade to the Internet Routing (discussed in Section 3.5) and Internet Content functions.
Concern	In general, an attack on the Internet-based function or its sub-functions does not require a high degree of skill or knowledge.
Impact	Mitigating risk to the *Provide Internet-based Content, Information, and Communications Services* function should not only be directed at the producers/providers of the function, but also to consumers.

The IT Sector produces and provides Internet-based content, information, and communications capabilities that are critical to the assurance of national and economic security and public health, safety, and confidence. The Internet is established and maintained by service providers and telecommunications providers that ensure the delivery of Internet-based content. Telecommunications providers lay and maintain the cable that forms the physical infrastructure of the Internet and establishes a large, unified network of computers, telephones, and other network-based machines. Public and private sector entities leverage Internet service providers to connect to this unified network and exchange content, information, and communications.

3.4.1 *Provide Internet-based Content, Information, and Communication Services* Attack Tree and Risk Profile

The IT Sector provides five sub-functions in support of the *Provide Internet-based Content, Information, and Communications Services* critical function. These sub-functions are:

- Provide and support critical national security emergency preparedness (NSEP) and Law Enforcement functions;
- Provide mapping and geospatial data and imagery services to support NSEP functions;
- Provide and operate critical Web search capabilities;
- Provide and operate critical e-Commerce and financial transaction services;
- Provide communications and collaboration services (e.g., VoIP conferencing, peer-to-peer [P2P], instant messaging [IM]); and
- SCADA communication.

To evaluate the threats, vulnerabilities, and consequences to the function, risk assessment SMEs consolidated the five sub-functions into three major sub-functions to focus the scope of the Internet Content attack tree (Figure 17).

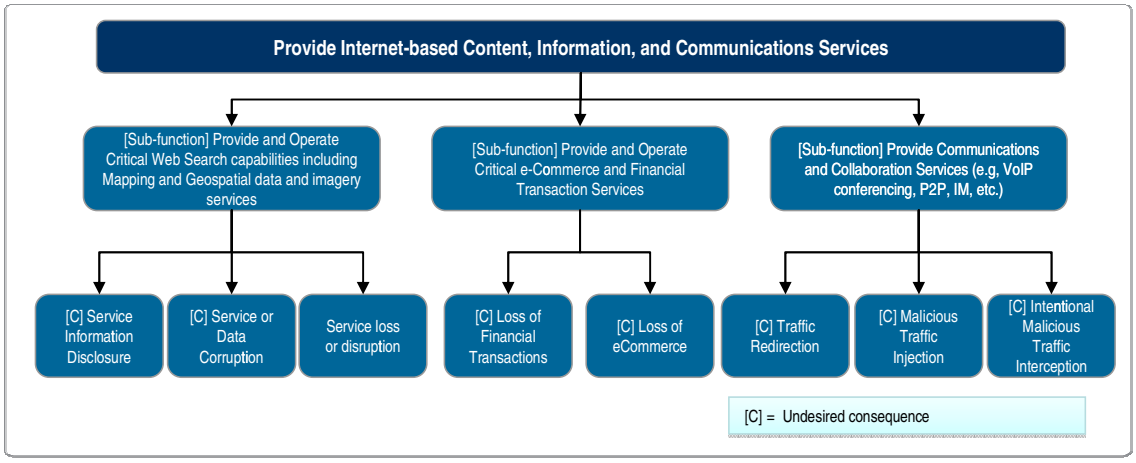


Figure 17: *Internet-based Content, Information, and Communications Services* Attack Tree (Summary)

Most threats to the Internet Content function result from cascading effects from an attack on the DNS or Internet Routing functions, though redundancies within those functions reduce the risk of these impacts. The Internet Content function is vulnerable due to its constant accessibility and exposure. The introduction of available and easily deployable malware kits only heightens this vulnerability. Consequences to an exploited vulnerability have the potential to significantly impact national and economic security and public health, safety, and confidence, but this is not very likely. Current mitigations typically focus on controlling policy and access rights within organizations, but this leaves the function vulnerable to entities outside of this sphere.

In general, a deliberate attack on the *Produce and Provide Internet-based Content, Information, and Communications Services* function does not require a high degree of skill or knowledge, and individuals, clubs, or teams are capable of successfully conducting attacks against the function. Manmade deliberate threat actors may have several motivations, including financial gain, especially with regard to the e-Commerce and financial transaction services sub-function; intelligence gathering, including state-sponsored, and corporate espionage; the desire to project power through capability demonstrations; or to deceive end users. In addition, most attacks require only limited logical access and few significant resources. More widespread and nationally consequential attacks require greater sophistication, perhaps from an organized crime syndicate or nation-state, and higher skill-levels.

Provide and Operate Critical Web Search Capabilities Including Mapping and Geospatial Data and Imagery Services

Critical Web search capabilities help end-users find specific information in the expansive Internet. Mapping and geospatial data and imagery services may use the Internet to provide geo-coded information for use in business and government applications. An impact to the Sector's ability to operate critical Web search capabilities, including mapping and geospatial data and imagery services, could cause significant and lasting national security and economic consequences as a result of:

- Service information disclosure;
- Service or data corruption; and
- Service loss or disruption.

Threats to this sub-function are typically the work of a deliberate threat actor leveraging algorithm disclosures or automated malware, which is software intended to damage the confidentiality, integrity, or availability of information on a system. Threats may also include phishing attacks, malicious redirects, and passive monitoring conducted through spoofed or counterfeit Web sites. Most of these threats focus on affecting confidentiality or integrity, but not availability. Availability is important to attackers, as it helps

minimize the likelihood that their intrusions will be discovered by end users. A threat actor would ideally want months to elapse before any exploitation is noticed, allowing for the collection of significant amounts of information. The victim will need to expend significant effort in recovering and verifying content. Many of the function's vulnerabilities relate to the processes and adherence to established security practices by the workforce. For example, organizations that do not enforce log audits leave themselves exposed to brute force attacks.

These concerns are valid for both enterprise and government content providers. For example, if the Internet Routing function is forced to re-route unencrypted Internet traffic through untrustworthy entities, such as ISPs that are located in a foreign country, the risk for information disclosure, data corruption or loss, or disruption of service increases. As with threats to the sub-function's confidentiality, exploited vulnerabilities related to the sub-function's integrity could take months to notice and leave in doubt the recovery of Web search and geospatial imagery services data. This is not very likely to occur, but it is noteworthy due to the strategic implications involved with national and economic security data being routed insecurely through unknown or untrustworthy entities.

Network infrastructure or back-end failures could also result in disruption of service, but this result would be much less likely the work of deliberate threat actors and more likely the result of unintentional or natural threat actors. Deliberate threat actors need the services to be available in order to undermine the confidentiality and integrity of those services as discussed previously.

Provide Communications and Collaboration Services

The IT Sector provides communications and collaboration services, including, video VoIP, e-mail, IM, P2P file sharing, and others. Exploitation of DNS, BGP,[37] and other routing protocol vulnerabilities could cause significant and lasting national security and economic consequences. The inability of the Sector to provide and operate critical communications and collaboration services would result in:

- Traffic re-direction;
- Malicious traffic injection; and
- Intentional malicious traffic interception.

As with the operation of critical Web search capabilities, including mapping and geospatial data and imagery services, threats to communications and collaboration services often revolve around the exploitation of confidentiality and integrity. These services may use different protocols and applications to operate, both of which are potential opportunities for exploitation. For example, the protocols or applications could have vulnerabilities that allow for the execution of malicious code, as was the case with several IM and P2P programs and VoIP software packages. These exploitations are generally specific and require significant knowledge of flawed software. Also, once the security vulnerabilities are realized, the providers of communications and collaboration services quickly try to address the vulnerabilities.

As with Web search capabilities, threat actors rely upon the constant availability of the sub-function in conducting attacks, which may include, re-directing Web traffic to spoofed or counterfeited Web sites, performing malicious traffic injections, or intentionally intercepting Web traffic. The concerns are broadly applicable because video VoIP, e-mail, IM, P2P, and other services play an integral part in the daily operations of many organizations. This level of connectivity to and reliance upon the Internet ensures that the impact of a successful attack on the function cascades to the end user. For example, disclosure of sensitive information, including payment or health information; denial of actions; and code injection would lead to consequences such as identity theft and damage to brand image. Additionally, it could take months to notice that vulnerabilities were being exploited, which can lead to significant revenue and intellectual property losses.

[37] For an evaluation of risks to the DNS, please see Section 3.2, *Providing Domain Name Resolution Services*. For a discussion of BGP, please see Section 3.5, *Providing Internet Routing and Connection Services*.

Nation-states and expert hackers are no longer the only threat actors targeting the sub-function. The introduction of "do-it-yourself" malware kits have enabled threat actors with little skill to execute attacks that were once limited to the realm of the highly skilled. This has led to an exponential rise in the number of threats to the function and, when combined with the function's constant accessibility and exposure, has created a parallel increase in the likelihood of a vulnerability being exploited. While the likelihood of exploited vulnerabilities may be on the rise, these exploitations are limited in scope and are not of national significance.

Failures or disruptions to other functions can also become threats to the Internet-based Content sub-functions. Consequences resulting from unintentional threats to the function can often be traced to the DNS or Internet Routing functions. Unintended BGP changes, or improperly updated BGP tables, can cause Web sites to be unreachable on a local or regional basis until the error is corrected. Disruptions in the routing function can cascade to the DNS function and on to the Internet Content function, thereby potentially making Internet content unreachable as well. Often these consequences impact availability, but if the Internet Routing function is forced to re-route Internet traffic through a foreign country, it raises the risk for traffic re-direction, malicious traffic injections, or intentional malicious traffic interception. The involvement of a foreign government would most likely be required to exploit this vulnerability, raising the strategic implications involved with national and economic security data being routed through a foreign country.

Provide and Operate Critical e-Commerce and Financial Transaction Services

The IT Sector provides and operates critical e-Commerce and financial transaction services on which citizens, businesses, and government entities rely to conduct their financial transactions. An impact to the Sector's ability to provide and operate these services could cause significant and lasting national security and economic consequences. The inability of the Sector to provide and operate critical e-Commerce and financial transaction services would result in:

- the loss of "instant" financial transactions and
- the loss of e-Commerce.

A denial-of-service attack on payment transaction companies could render these entities unable to conduct their operations. While the attack on the company itself may not be of national concern, the cascading effects on citizens, businesses, or governments could be of national or regional concern, especially when considering public confidence. Furthermore, attacks on the Identity Management function, and specifically identity certificates and credentials, could compromise financial transaction authorization, clearing, or settlement systems. Threat actors rely upon the constant availability of the sub-function in order to compromise financial transactions and e-Commerce. It could take months to notice vulnerabilities being exploited and confidence in the sub-function may never be fully recovered.

In addition to specific attacks on financial transactions, certain threats could disrupt the Nation's ability to conduct e-Commerce. For example, large scale DDoS, Web re-directs, or spoofing attacks could disrupt e-Commerce Web sites; Web spoofing or MITM attacks could enable actors to hijack user accounts and Structured Query Language (SQL) injections or cross-site scripting could enable payment card data to be compromised. For attacks like these, financial gain often motivates attackers. The internal testing of software could also lead to unintended negative consequences when the parameters of the test do not meet the reality of the intended environment. These consequences could pose a greater risk when the release of the software is combined with insufficient contingency plans. Availability could be affected, which could pose significant consequences to national and economic security, as well as public health, safety, and confidence.

Natural disasters, such as floods, earthquakes, and storms, would not directly impact the sub-function; however, natural events affecting other functions could potentially cascade to the sub-function. Severe or catastrophic natural events do occur and can impact the integrity and availability of the Internet Routing and Internet Content functions. Natural events affecting the Communications and Energy Sectors could also cascade to affect the Internet-based Content sub-functions. For example, power outages over

extended periods could result in communications disruptions or congestion, if facilities do not have backup power or fuel sufficient for the duration of the outage.

The threats and vulnerabilities posed to the Internet Content function are largely due to the high degree of human interaction associated with the function. Mitigations to the vulnerabilities raised by this human element include policy and access control, security training, and log audit enforcement with continuous review of the mitigations.

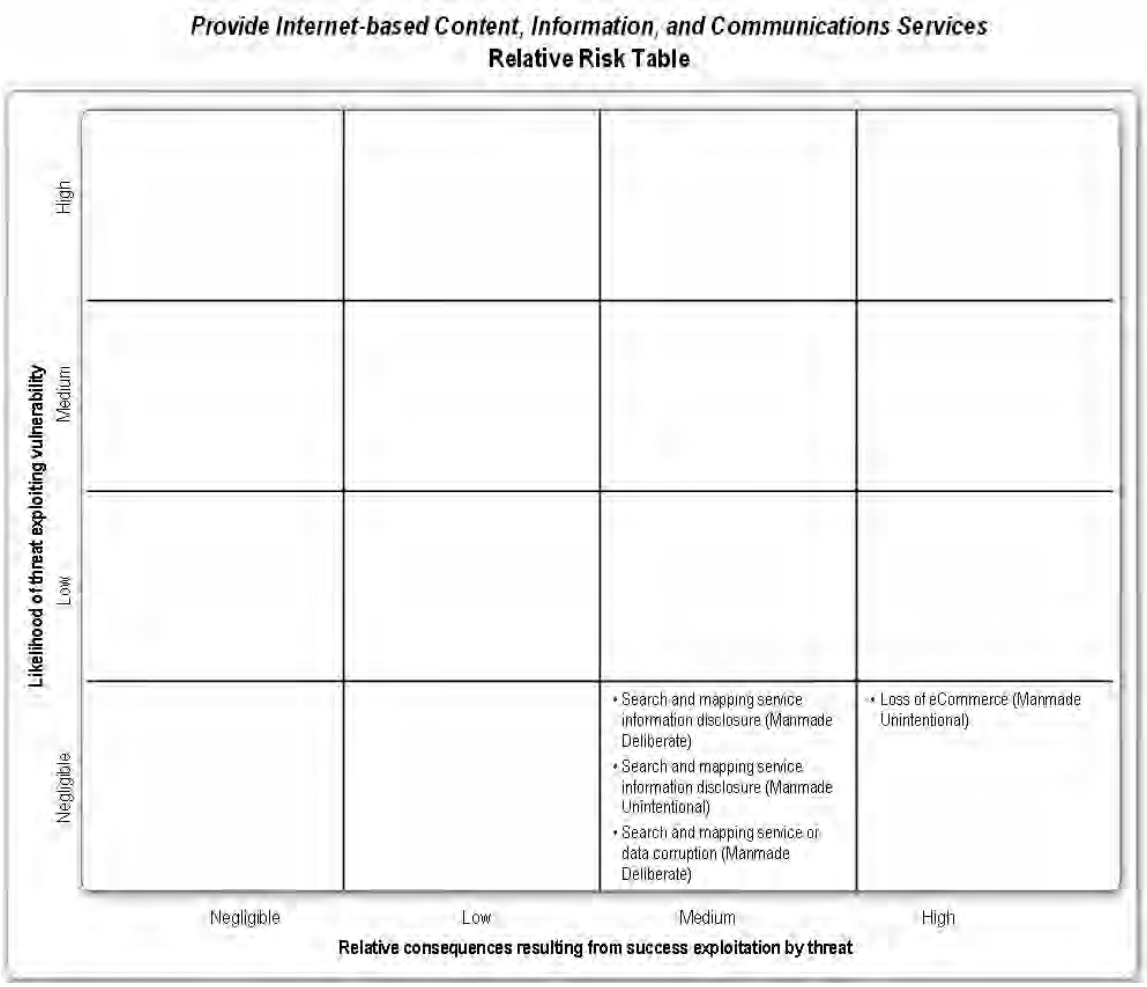


Figure 18: Relative Risks to the *Provide Internet-based Content, Information, and Communication Services* Function

3.4.2 Mitigations

As part of the Baseline Risk Assessment, the SMEs identified existing and future mitigations that address the risks outlined for the *Provide Internet-based Content, Information, and Communication Services* function. The mitigations were categorized as existing mitigations, mitigations currently being enhanced and improved, and future mitigations. These categories will assist the IT Sector outline R&D and protective program priorities

Existing Mitigations

- Terminating access controls: The proper implementation of policy and access controls provides the most widely available mitigation for threats to the Provide Internet-based Content function. Terminating access rights immediately after an individual leaves an organization is a common mitigation currently implemented within the function. Failure to terminate access leaves the organization vulnerable to information disclosure, the introduction of malicious content, or to a brute force attack against the organization's infrastructure. The termination of access rights provides a simple and effective way to mitigate the potential vulnerabilities posed by an individual leaving an organization.

Mitigations Currently Being Enhanced and Improved

- Least privileged access: Although it is becoming increasingly common to terminate the access rights of individuals that leave an organization, many organizations are improving the updating of access rights for users that transition internally. Individuals that transition within the organization could still have access to content that they do not, and should not, have the ability to access. Access to content not related to the assigned task could lead to information disclosure or the introduction of malicious content into the organization. Updating access rights to reflect internal changes provides a simple and effective mitigation to threat.

- Security training: Security training is an effective method for enhancing an overall security policy. Consistency among security training programs and practices across the IT Sector should be more widely adopted. Considerable funds are expended on achieving compliance standards, while more efforts focused on user education could augment and enhance the effectiveness of compliance driven approaches. Many individuals are unaware of, or fail to understand, the risks posed by threats to the Provide Internet-based Content function, raising the risk of unintended negative consequences. Proper and consistent security training, both at the national and organizational level, could mitigate many of the threats posed by these unknowing actors. In addition to specific security training, there are National-level cybersecurity awareness programs and organizations, such as the National Cyber Security Alliance, that seek to educate and inform home users and small businesses about the importance and impact of cybersecurity.

Potential Future Mitigations

- A comprehensive national training and education program targeted to all Internet users: While security training programs are being enhanced or improved, there is a need to integrate cybersecurity throughout all aspects of users' activities. A flexible, comprehensive, and sustained security training and awareness program at the national-level—that begins when individuals enter the education system and continues throughout their professional and personal activities—could mitigate many of today's threats to the Internet Content function.

- Enhance rerouting capabilities of the Communications and IT Sectors: Both sectors should continue to work together to provide alternative means to quickly redirect Internet traffic during an outage to ensure the constant availability of the function for all users.

3.5. Provide Internet Routing, Access, and Connection Services

Provide Internet Routing, Access, and Connection Services Function Summary	
Situation	The distributed nature of Internet facilities and the adaptability of packet switching make the Internet particularly resilient, but not immune to attacks and outages. The concentration of physical assets supports a narrow range of physical threats to the function.
Concern	Threats to BGP and other interdomain router operating systems and intra-domain protocols are the primary vulnerabilities within the Internet Routing, Access, and Connection Services function.
Impact	Internet network operators and ISPs are regularly targeted by attackers who attempt to disrupt Internet routing with DoS attacks, DNS cache poisoning, and BGP route hijacking.

The IT Sector provides Internet routing, access, and connection services capabilities that underpin, and are therefore critical to the assurance of national and economic security and public health, safety, and confidence. The IT Sector, in close collaboration with the Communications Sector, provides and supports Internet backbone infrastructures, points of presence, peering points, local access services, and capabilities to direct Internet traffic.[38] Efficient Internet traffic routing ensures that information is delivered to end users by the most expedient means possible.

The Internet Routing critical function has seven sub-functions. These sub-functions are:

- Provide and operate critical collocation facilities and carrier hotelling;
- Provide and operate critical Internet exchange fabric;
- Provide and operate critical local access capabilities;
- Provide and operate critical Internet backbone/core services and capabilities;
- Provide routing/peering security operations and incident management;
- Provide and support critical NSEP and law enforcement functions; and
- Provide address and Autonomous System Number (ASN) allocation services.

3.5.1 Internet Routing, Access, and Connection Services Attack Tree and Risk Profile

To evaluate the threats, vulnerabilities, and consequences to the *Provide Internet Routing, Access, and Connection Services* critical function, risk assessment SMEs structured the Internet Routing attack tree around three undesired consequences.

- Partial or complete loss of physical facilities and lines;
- Impairment of operations support and incident response/management; and
- Partial or complete loss of routing functions and supported services.

[38] Adapted from the Information Technology Sector Specific Plan (IT SSP), May, 2007.

The distributed nature of Internet facilities and the adaptability of packet switching make the Internet particularly resilient, but not immune, to attacks and outages. Risk assessment SMEs identified the concentration of physical assets and threats to BGP, operating systems, and intra-domain protocols as vulnerabilities to the Internet Routing function.

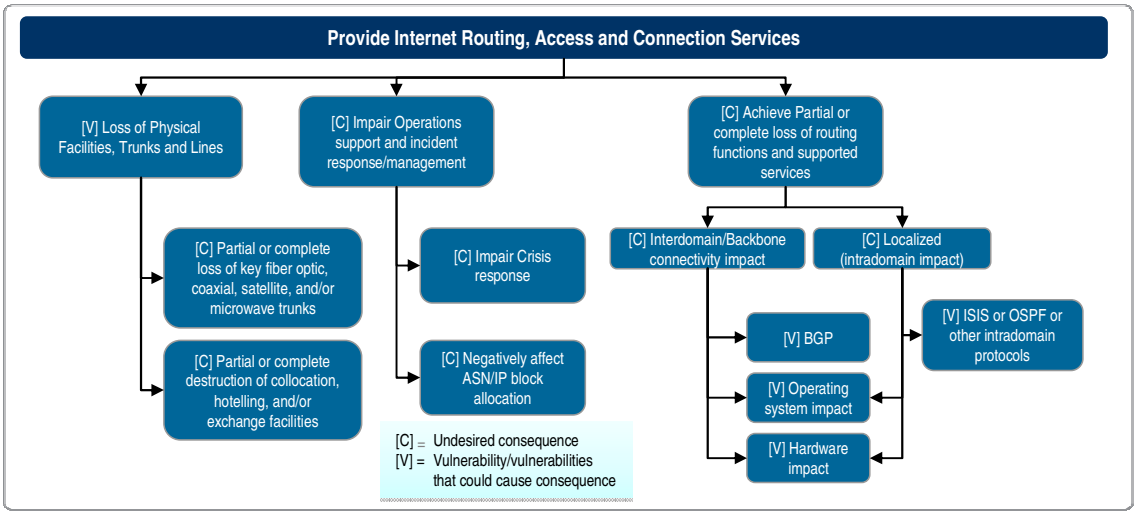


Figure 19: *Internet Routing, Access, and Connection Services* Function Attack Tree Summary

Loss of Physical Facilities, Trunks and Lines

Complete loss of Internet routing infrastructure is unlikely due to the intentionally distributed nature of its physical and operational underpinnings, but varying degrees of impact could be caused by localized damage at specific portions of the routing infrastructure. Damage to hardware and facilities supporting the network and the concentration of infrastructure within exchanges, collocation, and hotelling environments could cause significant and lasting national security and economic consequences.

Risk assessment SMEs identified two key areas of focus regarding physical damage or loss to the *Provide Internet Routing, Access, and Connection Services* function:

- Partial or complete loss of key fiber optic, coaxial, satellite, and/or microwave trunks; and
- Partial or complete destruction of collocation, hotelling, and/or exchange facilities.

Risks to the Internet routing function include outages to communications links caused by construction, excavation, or accidents. For example, consortia of private sector entities typically share the costs of and own rights to access the undersea cables linking worldwide and intercontinental networks. Cables lie on the ocean floor exposed to ships' anchors, which have cut transoceanic cables in the past. The consequences of a severed cable could have an immediate impact, though not necessarily severe, on Internet availability to particular regions of the world. The durations of such impacts could also vary. In addition, all of the functions that rely upon Internet routing, such as the DNS and Internet Content functions, would be affected.[39] National and economic security and public health, safety, and confidence missions that are dependent on services routed through the severed cable would be impaired, and the consortia that own the cable would face substantial repair costs.

[39] For an example of such an incident, please see the *Los Angeles Times* article from February 1, 2008 by Michelle Quinn entitled "Undersea cable accident a test of the Internet" http://articles.latimes.com/2008/feb/01/business/fi-india1.

There is a relatively narrow range of threats that could cause the loss of physical elements of this function. In general, an attack against the *Provide Internet Routing, Access, and Connection Services* function would require capabilities that only a government or organization could provide (relative to an individual or group). Although an insider with access to key parts of the function's infrastructure would have limited time and funding to execute an attack, it is possible for an individual to facilitate or execute an attack.

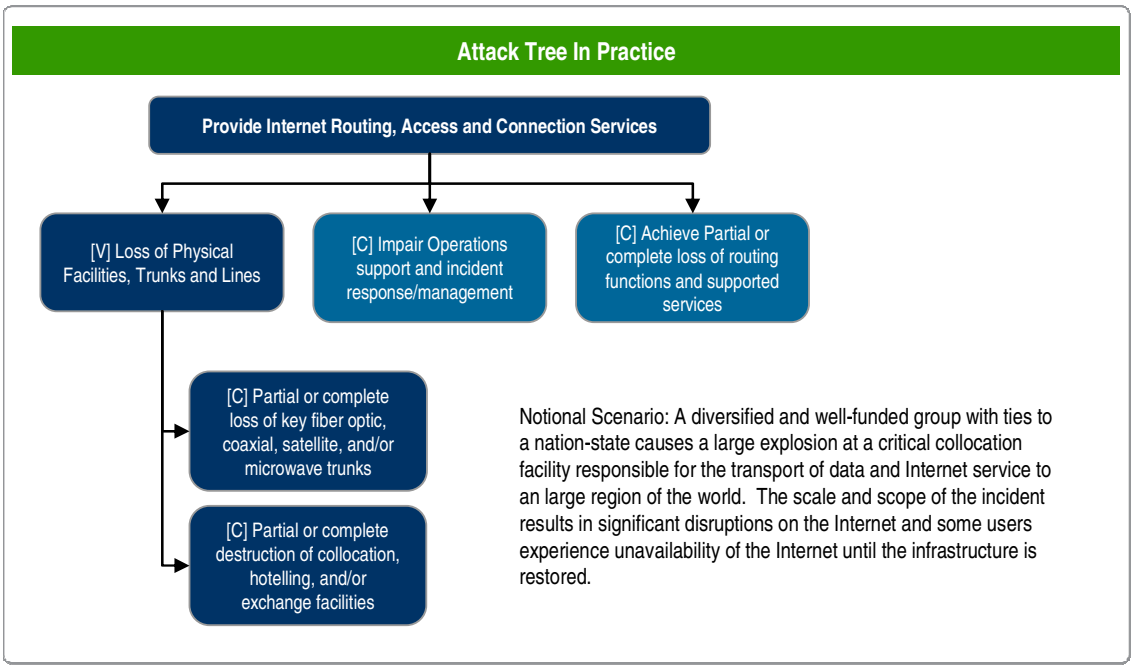


Figure 20: Notional scenario applied to the *Provide Internet Routing, Access, and Connection Services* Attack Tree

The Internet routing infrastructure is composed of many networks grouped into Autonomous Systems (AS) that are interconnected. Each AS is controlled by a single administrative entity, such as an ISP, a business enterprise, or a government organization. An AS can range in size from a small collection of routers in a room to a nationwide backbone network run by an ISP. Although many ISP backbone networks may be in a single AS, some networks can consist of multiple AS due to size, acquisition and network build-out strategies.

In some cases, a failure that causes a local or regional disruption could lead to national consequences. However, there are currently no real world examples in the United States due to mitigation strategies that providers implement. The closest example in the U.S. was the service disruptions in lower Manhattan that cascaded to degradation of service in the greater New York City area during and after the September 11, 2001 terrorist attacks; nevertheless, the Internet continued to operate throughout the country.

Natural disasters, such as floods, fires, and storms, can also affect the operation of routing centers and interfere with Internet routing. Although most Internet routing centers are housed in secure sites with their own emergency power generators, high risk locations, such as areas susceptible to regularly-occurring natural disasters, are a significant vulnerability that would require planning and investment to mitigate. Although catastrophic natural events are relatively rare, it is when these events occur that the availability of the function is paramount. Even if the physical site could withstand a catastrophic natural event, operations may prevent personnel from physically reaching the site to respond to the incident. However, the resiliency and redundancy of these physical and logical infrastructures mitigates many of the associated risks.

Natural disasters can also affect the communications links between Internet routing centers. For example, undersea earthquakes have been known to set off undersea landslides that sever submarine communications cables. In all the cases above, Internet routing protocols will quickly re-direct traffic around the outages if an alternative route exists. However, there could be traffic congestion or short-term disruptions of the service until the traffic is fully re-directed and the links are restored.

Impair Operations Support and Incident Response/Management

Operations support and incident response/management are crucial for maintaining operations and responding to problems expeditiously. The network architecture and design within which BGP operates must take into account matters such as peering and security. It is the responsibility of network designers and operations support personnel to ensure that the correct functional features (such as route filtering) are utilized to realize secure and correct network operation, and to provide human oversight to automated functioning. Router configuration is often automated but there is room for error either when new equipment is installed or because particular versions of software or product templates may be incorrect. For all these reasons, it is important to have adequate operations coverage by staff capable of performing these tasks.

BGP is the protocol used to connect multiple networks on the Internet. Because BGP relies on peering and is a contract or policy-based routing protocol, the expense and difficulty involved in the daily management of BGP filtering and security are factors that contribute to the overall vulnerability of the function. BGP vulnerabilities can leave the routing network susceptible to BGP shunting/hijacking, especially those inherent to operating inter-domain policy, and create “blackholes,” which would allow actors to re-direct and/or intercept, eavesdrop, or drop traffic. Thus, BGP filtering and security are an important part of operations.

Another key area of focus regarding the impairment of operations support and incident response management is exchange point operations. These points are vulnerable to manmade and natural threats. The operations of most routing centers may be, and frequently are, monitored remotely, but technicians must be able to reach the site to respond to an outage or an incident. Manmade and natural threats may prevent access to these facilities and could lead to an impairment of the Internet routing function.

Major ISPs do take precautions to prevent disruption of operations support and incident management/response. Most major providers have several backups for all of their routers, so if one router were to go offline, there would be an immediate failover. The backup would continue to operate until another incident occurred. Monitoring changes to software is of greater concern than monitoring router hardware for failure, but most ISPs and network operators take significant precautions in deploying new software and conduct testing followed by phased deployments.

Impacts to the function’s confidentiality and integrity could occur if data is being relayed through points outside of the U.S. This puts the integrity of the data at risk of being leaked or otherwise altered. The redundancy built into the function limits this likelihood, but there are strategic implications involved with national and economic security for data routing through foreign countries. Data encryption at the application layer using certificates would provide one approach that is independent from this function that could also serve as a mitigation to some of its risks.

Partial or Complete Loss of Routing Functions or Sub-function(s)

Whereas the impact from physical damage to routing facilities is limited to local or regional areas, the impact from an attack on a routing protocol could have wide-spread, nationwide and global effects. The common strategic objectives identified with impacts to the routing functions or sub-functions are obstruction and financial or technical gain, with the intended outcome of such attacks being theft or acquisition of data. A partial or complete loss of key Internet routing trunks, facilities, and/or functions and supported services through malicious or accidental manipulation of routing protocols and associated network/equipment configurations could cause significant and lasting national security and economic consequences.

Risk assessment SMEs identified two key areas of focus regarding the loss of routing functions: (1) Inter-domain/Backbone connectivity impact and (2) localized, intra-domain impact. The focus in this section, due to its potential for widespread impact, is on inter-domain protocol attacks.

Although no single AS is connected to every other AS, some backbone networks are large enough that many smaller networks depend on them to reach the rest of the Internet. For example, a local ISP providing service to a small community may connect to a larger AS with a nationwide backbone for national connectivity. These AS relationships constitute a complex hierarchy.[40]

Customer organizations access the Internet by purchasing connection agreements to an ISP, and are allocated an IP address for the duration of the agreement.[41] These connections are terminated into access routers owned and operated by the ISP. The access routers, with other backbone equipment, are contained at a site known as a Point of Presence (POP). POPs are usually located within an ISP's data centers or collocation facilities. A Tier 1 network provider, which is a network with direct connections to other networks on the Internet, may operate POPs in many major cities. Most customers become a part of an ISP's AS when they connect to one of the ISP's POPs. Figure 21 illustrates a simplified view of inter-ISP connections and IS' connections to Internet backbone networks.

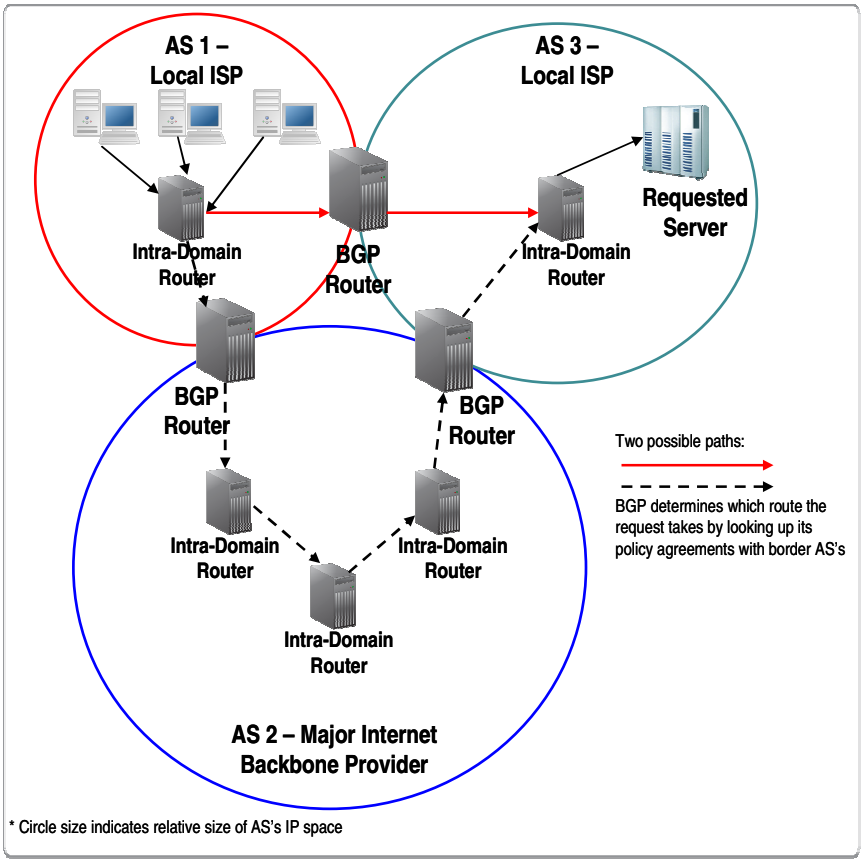


Figure 21: Internet connections between AS and backbone networks

[40] Interconnection points between some ISPs are known as peering points or Internet exchange points (IXP).
[41] Greene, Barry Raveendran. Smith, Philip. "BGPv4 Security Risk Assessment". The ISP Essentials. Version 0.3. Cisco Press. June 2002.

ISPs have collections of routers that run a variety of routing protocols. The routers vary in their technical sophistication and packet processing speeds, and the routing protocols must be configured to operate correctly and efficiently.

Internet routing and packet switching were initially designed for military network use to account for situations in which parts of the network could become unusable or inaccessible. Flexible routing and switching protocols were developed to allow access to the network even while some parts were inaccessible. This capability was carried forward as the Internet evolved into a system that could serve both business, military, and civilian uses.

The primary routing protocol used in AS is BGP, and BGP connects routers in different autonomous systems. At a very basic level, BGP is a protocol routers use to determine routes to Internet destinations. A routing disruption occurs when an attacker compromises a router and causes it to send out false routing information to other routers. Depending on the router location in the network, a compromised router could perpetuate incorrect routing information throughout the Internet.

False routing information can misdirect traffic and cause congestion. A "blackholing attack" refers to a phenomenon when all inter-AS traffic for a specific network between AS to a particular destination is directed toward the compromised router and then discarded. One example of "blackholing" occurred in 1997, where a small ISP in the U.S. propagated bad routing information to a major ISP resulting in widespread disruption within the Internet. Recently, an ISP in a nation trying to block its citizens' access to YouTube inadvertently "blackholed" most YouTube traffic worldwide. The ISP broadcast incorrect BGP routing information about the network addresses on which YouTube servers were located, directing YouTube traffic to its "blackholed" routers.[42]

These examples illustrate that Internet routing is vulnerable to instability or incorrect operation caused by errors in routing announcements by ISPs and backbone providers, as well as unintended mistakes in how routing announcements are handled by ISPs. ISPs "peer" with one another, subject to specific peering agreements which amount to cooperative agreements to carry traffic to legitimate network addresses as decided by the business arrangement. However, there is no central operating authority for the Internet, and there are few effective controls on what one ISP announces to its peers. Without an authoritative source to validate which network providers can provide transit to specific traffic, few network operators conduct inter-provider address and route filtering.

Providers large enough to be a "peer" do not want to be seen as the source of bad routing information that affects delivery of global e-mail traffic or blocks access to Internet content. This system of self-regulation does not deter hackers and other deliberate attackers who want to disrupt the Internet routing function by targeting network operators and ISPs. However, ISPs and network operators surveyed in the Arbor Networks' 2007 World Infrastructure Security Report (WISR) believe that they have the capability to effectively mitigate against most of the attacks aimed at themselves and their customers.[43]

Most DoS attacks tend to be brute force attacks that try to flood a provider with extraneous traffic by taking down one or more routers. Network operators have tools and techniques to handle these problems. According to the Arbor Networks report, many operators credit improved information sharing with other operators, as well as the work of in-house security teams, with their ability to control the risk. In the 2008 WISR, ISPs surveyed expressed increased concern with DNS cache poisoning, unintentional and malicious BGP route hijacking, and bots and botnets. The report also noted that for the first time, the size of DDoS attacks scaled up as high as 40 gigabytes per second (Gbps), hundreds of times larger than

[42] Sone, Brad. "Pakistan Cuts Access to YouTube Worldwide". *The New York Times.* February 26, 2008. http://www.nytimes.com/2008/02/26/technology/26tube.html
[43] Arbor Networks. "Worldwide Infrastructure Security Report". Vol. III. September 2007. http://www.arbornetworks.com/report

what they were in 2000, and continue to outpace the corresponding growth in transmission speeds and ISP infrastructure investment.[44]

Unintentional incidents resulting from errors and mistakes by network operators also pose a threat to Internet routing. Examples include errors in configuring routing protocols or oversight resulting from inadequate monitoring of equipment, traffic loading, and router and communications link status at IXPs and Network Access Points (NAP). The internal nature of these errors has created a constant vulnerability to threats that are not always easy to identify until after the consequences have been realized. An impact to the function's availability will be the most likely consequence of an unintentional threat. Unintended BGP changes, or software defects that cause delayed or stale routing data, can have immediate, cascading effects on a global scale. Impairment of national and economic security and public health, safety, and confidence could continue until the errors are corrected.

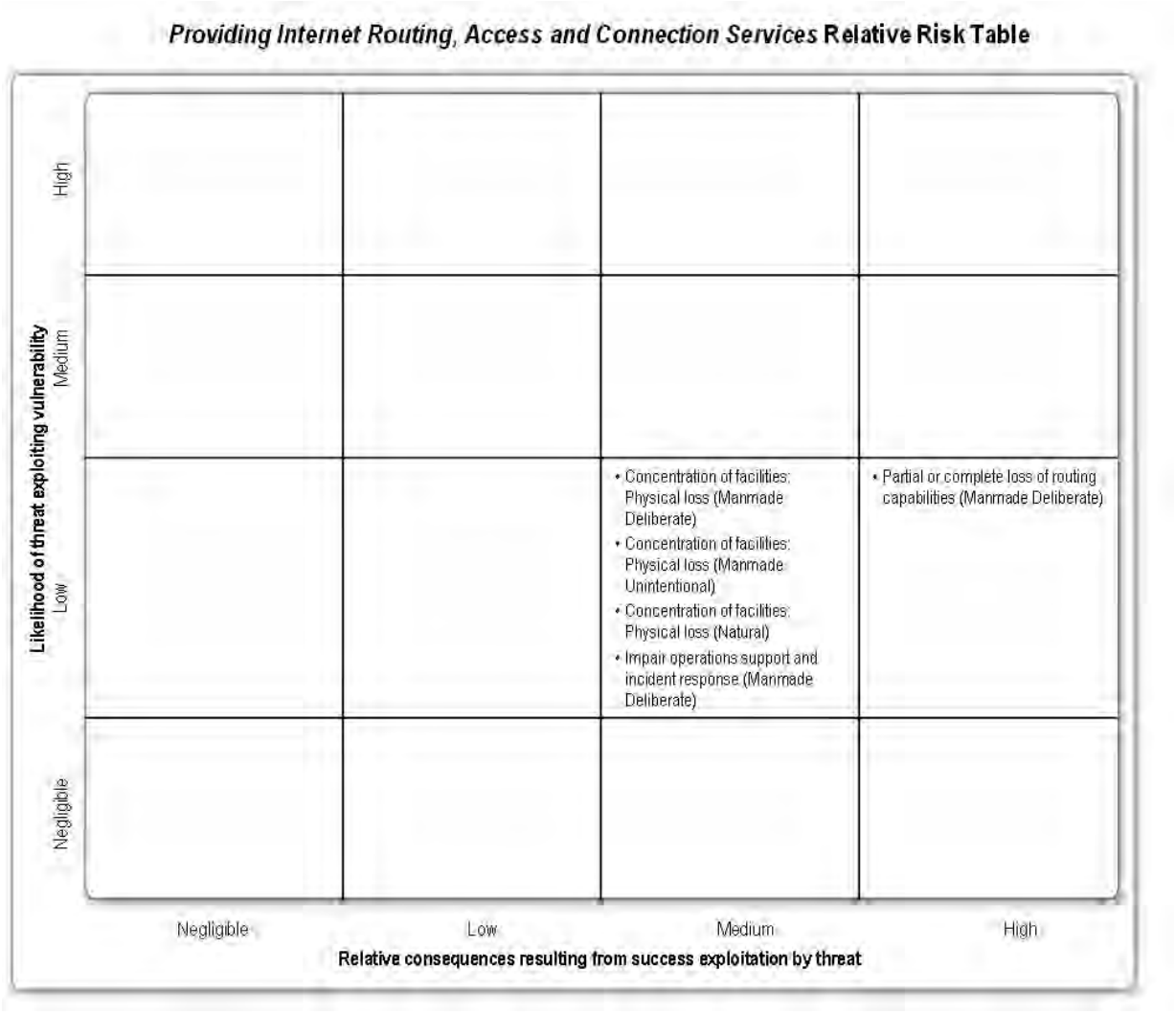


Figure 22: Relative Risks to the *Provide Internet Routing, Access and Connection Services* Function

[44] Arbor Networks. "Worldwide Infrastructure Security Report". Vol. IV. October 2008. http://www.arbornetworks.com/report

3.5.2 Mitigations

As part of the Baseline Risk Assessment, the SMEs identified existing and future mitigations that address the risks outlined for the *Provide Internet Routing, Access and Connection Services* function. The mitigations were categorized as existing mitigations, mitigations currently being enhanced and improved, and future mitigations. These categories will assist the IT Sector outline R&D and protective program priorities

Existing Mitigations

- Enhanced routers: Dramatic increase in Internet traffic has prompted router manufacturers to increase the speed, reliability, and capacity of their routers and router software.

- Protocol redesign and enhancement: The most widely used routing protocols, such as BGP, Intermediate System - Intermediate System (ISIS), and Open Shortest Path First (OSPF), have been modified or enhanced to improve their efficiency, even as the number of Internet destinations has grown. These improvements offer redundancy and inherent resiliency built right into the function itself.

- Information sharing: The North American Network Operators' Group (NANOG) is a technical support forum for ISPs and network operators. The group's members perform an important risk mitigation role for the global Internet. In addition to sponsoring technical presentations at its three-times-a-year regular meetings of members, NANOG maintains an extensive library of technical support resources for ISPs and network operators. It also sponsors e-mail lists in which network operators can discuss network problems and get assistance resolving routing and connectivity issues.

- Community of practice: As a group dedicated to the role of the network operators, NANOG members play the most prominent roles in mitigating Internet routing problems. Other technical groups, such as the International Engineering Task Force (IETF), Réseaux IP Européens (RIPE, or the "European IP Networks"), Internet Assigned Numbers Authority (IANA), and American Registry for Internet Numbers (ARIN), also play a role in establishing standards, sponsoring R&D of new and improved technologies, and providing support to network operators.

Mitigations Currently Being Enhanced and Improved

- Responsiveness to increasing Internet traffic: Organizations that are responsible for Internet routing protocols, IP address assignment, and backbone communications engineering continue to respond to the challenges of handling the rapid increase in Internet traffic by devising standards, technologies, and techniques to make the Internet more resilient to failure. As has been noted, the IETF establishes standards and best practices, and ARIN promotes efficient assignment of IP address blocks, which reduces the size of Internet routing tables. There are other operating groups set up just for ISPs, such as NSP-sec lists.[45]

- Router performance: Router hardware manufacturers are responding to router performance challenges by developing new architectures in both processors and software to route more packets in the same switching fabric. At the same time, they are enhancing the security of routers by building in better protections against viruses and malicious code. They are also integrating more comprehensive network and device management capabilities into routers, so that they can be managed and monitored more easily at a central location.

[45] NANOG 29 NSP-SEC BOF, Keieo/Greene.

- Increase physical security of NAPs and IXPs: NAPs and IXPs continue to enhance and increase their security. The owners and operators of these facilities regularly collaborate with government to address the changing and evolving risk landscapes at each facility.

- Configuration management and testing: Organizations take significant precautions in deploying new software and conduct significant testing followed by staged deployments, to prevent unintended software change defects that cause delayed or stale routing data. However, it is important that internal software parameters for testing consider the reality of the intended environment in order to prevent unintended negative consequences.

- Route dampening: When networks receive updated routing announcements from other AS, they employ route dampening techniques to minimize the changes that are made to BGP routing tables, which enhances routing table stability.[46]

- Multiplicity of peering arrangements: In an attempt to bring greater route diversity, redundancy, and resilience to their networks, ISPs and network operators have increased the number of peering arrangements and the geographic diversity of their networks.

Potential Future Mitigations

- More efficient route filtering: ISPs and network operators have expressed an interest in route filtering on routing table updates received from neighboring or peer networks, but few network operators do it. Identifying bad or maliciously propagated routes is difficult until after they have caused a network disruption. An erroneous routing announcement may be withdrawn, but it may take hours for corrected routing information to propagate throughout the Internet. Governments and network support groups may want to sponsor research into coordinated route filtering techniques.

- Secure BGP: Proposals have been made for AS operators to transmit digitally signed route authentication and authorization announcements. However, operators currently trust other operators' route announcements explicitly unless they have reason not to do so. The Secure BGP (S-BGP) approach uses PKI cryptography to ensure that a router cannot fabricate BGP route information. However, PKI is difficult and expensive and can adversely affect router performance if not maintained correctly. A similar proposal for Resource PKI (RPKI) would validate the originator of BGP route advertisements.[47] A simpler start might be to use IP Secure (IPsec) to secure BGP route announcements, as an incremental step to a more comprehensive security approach. In any case, operator training will be required to teach best practices for configuration, deployment, and operation of new security features.[48]

[46] Internet Service Provider Working Groups. "Consolidated Recommendations for Securing the Internet". National Security Telecommunications Advisory Committee. May 2002.
[47] D.R. Kuhn, K. Sriram, and D. Montgomery, "Border Gateway Protocol Security", NIST Special Publication 800-54 (Guidance Document for the Telecom Industry and US Government agencies), July 2007. (http://w3.antd.nist.gov/pubs/BGP_Security_Recommendation_SP800-54_July2007.pdf); Penn State University. "A Survey on BGP Security" April 2005 (http://www.patrickmcdaniel.org/pubs/td-5ugj33.pdf)
[48] Internet Service Provider Working Groups. "Education and Training Implications". National Security Telecommunications Advisory Committee. May 2002.

3.6. Provide Incident Management Capabilities

Provide Incident Management Capabilities Function Summary	
Situation	Threats to the *Provide Incident Management Capabilities* function are varied and typically occur in parallel to attacks on other elements or functions of the IT infrastructure. Depending upon their severity, attacks on IT Sector critical functions have the potential to deny or degrade the Sector's ability to detect, respond to, or recover from an incident.
Concern	Attacks against the incident management function could be force multipliers. This effect could increase the consequences of more traditional attacks against the IT Sector by inhibiting an effective response
Impact	Integrating lessons learned into future incident response procedures, policies, and prevention activities facilitates continuous improvement and fosters improved prevention and protection practices.

The IT Sector develops, provides, and operates incident management capabilities that are essential or critical to the assurance of national and economic security and public health, safety, and confidence. The *Provide Incident Management Capabilities* function includes capabilities to coordinate efforts to detect, contain, resolve, and recover from incidents. Furthermore, analysis of lessons learned throughout each incident management life cycle phase enhances security partners' preparedness and prevention capabilities.[49] The Sector's incident management capabilities are consumed by entities both internal and external to the Sector. Thus, elements of this function mitigate the overall risk to the other five critical functions. In addition, many of the capabilities provided by incident management service providers are conducted within individual entities. The scope of this assessment is focused on operations that provide this service to other consumers; it does not measure the effectiveness of IT organizations' organic incident management capabilities.

Supporting the incident management function are five sub-functions provided by the IT Sector. These sub-functions are:

- Provide preventive guidance, best practices, simulation, and testing;
- Provide and operate indications, alert, and warning capabilities;
- Provide and operate operation centers and teams;
- Provide and participate in information sharing, situational awareness, and information fusion activities; and
- Coordinate and provide response, recovery, and reconstitution.

Public and private sector coordinate to provide these five sub-functions. Because the private sector can quickly focus on requirements and needs, it often takes the lead in developing and deploying innovative incident management solutions, increasing the skills and availability of security professionals, and developing products and services that are responsive to the rapidly changing threat environment.

[49] From IT SSP, May 2007.

Function and sub-function mitigation activities focus on the incident management lifecycle illustrated in Figure 23. First, incident management providers proactively manage risk to their own operations and those of their customers. These prevention activities are performed through constant monitoring and mitigation activities designed to prevent daily incidents from becoming significant disruptions to systems, networks, and functions. Prevention efforts are advanced by using a variety of means, including the development and communication of protection strategies which organizations can implement to secure their networks and systems. Prevention and protection are further enhanced by IT Sector efforts to conduct operations and services that support the production of security services, such as penetration testing, risk assessments, and system testing. Although prevention and protection strategies and approaches do enhance the security of organizations, successful attacks are possible. Therefore, to improve response and recovery operations, the IT Sector provides detection capabilities and tools, so attacks against organizations' assets, systems, networks, or functions are identified as early as possible. These efforts improve response and recovery operations and overall risk management efforts. Detection is performed through a variety of means, such as technological solutions and human interaction, and it is enhanced by inter-organizational information sharing. For example, many IT Sector entities provide incident management capabilities and services, but they often do not operate independently. Instead, they cooperate and share data, through organizations such as the IT-Information Sharing and Analysis Center (IT-ISAC), which enhances the IT Sector's overall ability to detect and respond to malicious events. The threat information and analysis gained through this information sharing approach enables increased awareness of threats, enhancing response actions. Continued coordination between the public and private sector is needed to effectively provide incident management capabilities.

Figure 23: Incident Management Lifecycle

Response to an event includes the use of backup and recovery techniques; data retention and archiving; capacity management; and continuity of operations (COOP) plans. Like many other sectors, the IT Sector also supports response, recovery, and reconstitution through corporate social responsibility and community support activities, which occur at many levels (e.g., international, national, organization, and volunteer). In addition, the Sector provides operations centers and teams to coordinate and conduct crisis management operations.

After the Sector has responded to an attack and mitigated the consequences, it provides services that enable the recovery and reconstitution of the affected assets, systems, networks, and functions. To complete the incident management lifecycle, objective and subjective lessons learned data are recorded regarding each incident. This data serves to:

- Identify the processes, procedures, and policies that were and were not effective during the incident prevention, detection, response, and recovery stages of the incident management lifecycle;
- Update incident response policies and procedures based on successes and failures of previous incident response activities;
- Develop new prevention techniques, improving the overall incident management lifecycle for future attacks. For example:
  - Training and awareness;
  - Mechanisms to integrate incident lessons learned into subsequent product and service design and development; and
  - Improved testing procedures based on known vulnerabilities and threats.
- Improve information and intelligence flows between and across the public and private sectors to support the rapid identification of emerging cyber-related threats and other circumstances requiring intervention by government and private sector authorities.

When aggregated and used to inform future Sector-wide activities, lessons learned support the implementation of risk-based, information-driven prevention, response, and consequence management programs.

3.6.1 Incident Management Attack Tree and Risk Profile

Risk assessment SMEs used the incident management lifecycle approach to organize an attack tree and assess the risk to the incident management function. The attack tree focuses on four undesired consequences:

- Impact to detection;
- Impact to response;
- Impact to recovery; and
- Impact to mitigation and prevention of similar/same attack occurrence.

Risk assessment SMEs evaluated the attack tree against different threat categories (e.g., manmade-deliberate, manmade unintentional, and natural).

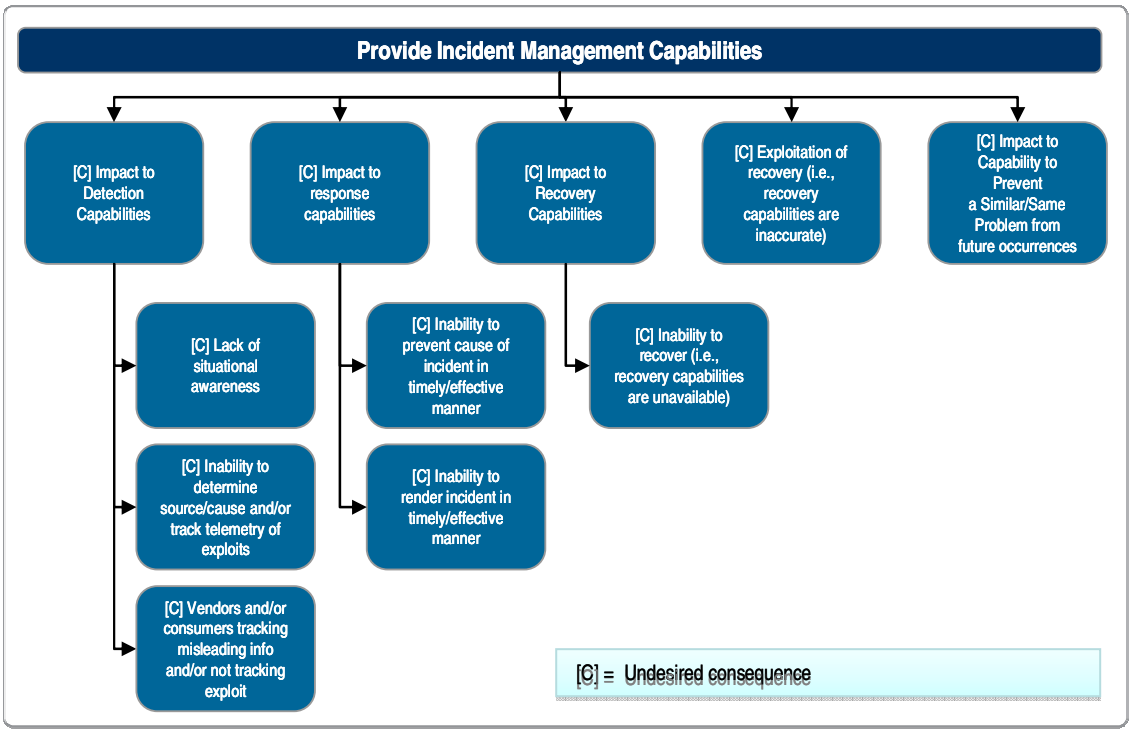


Figure 24: *Provide Incident Management Capabilities* Function Attack Tree (Summary)

Threats to the *Provide Incident Management Capabilities* function are varied and typically occur in parallel to attacks on other elements or functions of the IT infrastructure. Depending upon their severity, attacks on IT Sector critical functions have the potential to deny or degrade the Sector's ability to detect, respond to, or recover from an incident. These attacks may serve as force-multipliers for an attacker, increasing the consequences of more traditional attacks against the Sector by inhibiting an effective response.

Risk assessment SMEs identified various motivations for attacking incident management capabilities, such as financial gain, intelligence gathering, or political projection. However, regardless of motivation, such attacks are possible with operational-level skills, logical and/or physical access, and minimal resources. The types of actors can range from individuals internal or external to the Sector to more sophisticated organizations or—possibly—nation-states that are not bound by U.S. moral or legal code. Disgruntled employees could also implement attacks against the *Provide Incident Management Capabilities* function, highlighting the insider threat.

Unintentional threats to the function may come from employees or third party vendors, who generally are not as well trained as internal employees. These actors' roles in this function would likely be in implementation, production, and manufacturing; requirements, design, R&D, and discovery; or delivery, deployment, and distribution.

Common threat characteristics include significant physical access to the function's assets, systems, and networks; and the likely use of a defective, misaligned, or an un-calibrated tool.

Natural threats include those that could impact personnel and manufacturing such as epidemics or pandemics, droughts, and severe weather. Anything that affects the ability of the function to be adequately staffed is considered a threat.

Impact to Detection

A sustained failure to detect attacks could cause significant and lasting economic and national security consequences. Three main situations could cause this type of impact:

- A lack of common situational awareness among incident responders could leave critical assets, systems, networks, and functions vulnerable. This lack of situational awareness could be due to natural threats that prohibit key response personnel from accessing key incident data.
- The inability to determine the source, the cause of an attack, and/or to track the telemetry of exploits. Several vulnerabilities could exacerbate these concerns, including a lack of data to analyze if the incident is not being tracked; a lack of sharing and trending of data across the Sector and with other sectors; a possible gap in 24-hour incident management capability (a.k.a. "follow the sun" capability); a lack of availability of incident handlers and technical responders caused by manmade or natural events; and inaccurate or untrustworthy data used in incident detection.[50]
- Incident responders mistakenly using misinformed or inaccurate data to track and trend an event. This could be caused by trusting falsified reports or individuals as well as a lack of adherence to established data collection and analysis processes.

Due to the more visible and consumer-facing nature of this function, the consequences of a successful attack would typically be detected in hours or days; however, the source of the attacks may be difficult to determine. Detection is the first line of defense against active exploitations; any impact to the ability to effectively perform this mission would potentially have significant consequences.

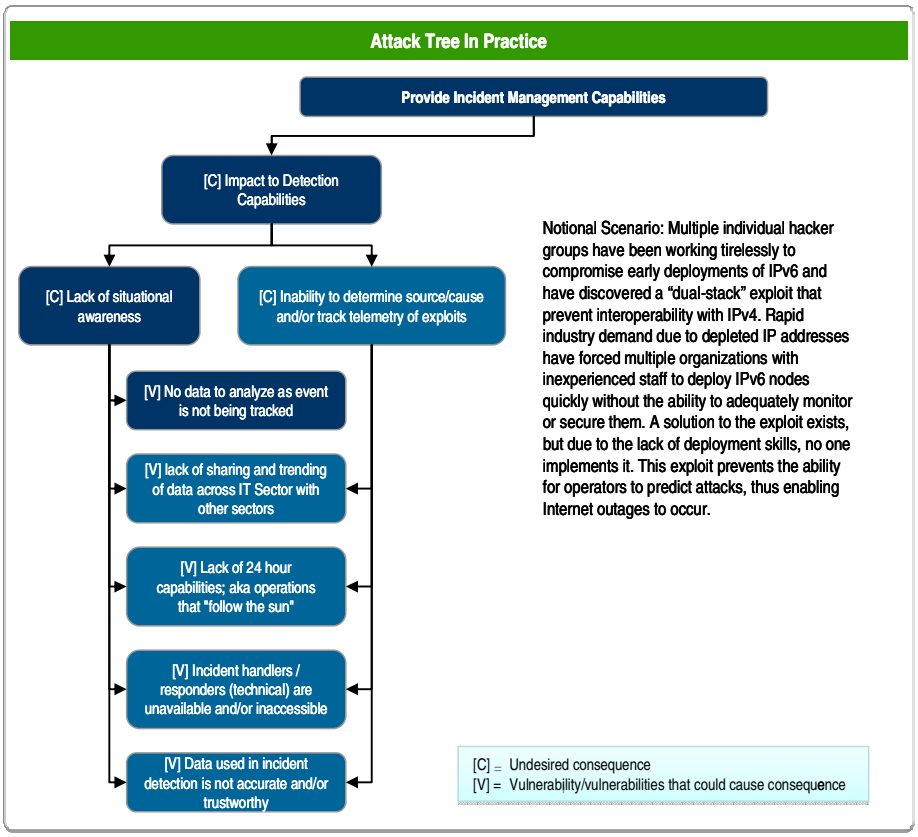


Figure 25: Notional scenario applied to the *Provide Incident Management Capabilities* Attack Tree

[50] These vulnerabilities are neither comprehensive nor prioritized by severity.

Impact to Response

Similar to an impact to detection, an impact to response could serve as a force-multiplier of a malicious attack. There are two primary concerns that may cause this type of impact:

- The inability to prevent; and
- The inability to contain an incident in a timely or effective manner.

These two concerns could be realized if the Sector cannot create and implement effective mitigations. The inability to communicate findings, therefore preventing proactive protective measures to be put into place, could allow for cascading impacts. The effectiveness of the Sector's response capability relies on the communications infrastructure, which includes human resources. Concentration of these resources is a potential vulnerability.

An inability to respond to malicious attacks through broad collaboration could cause both localized and nationally significant consequences. For example, an Internet worm can be effectively mitigated, if response is coordinated and conducted across all users by the successful patching of all systems and networks. Without this ability, consequences could worsen through the exponential propagation of the malicious code.

Impact to Recovery

The ability to quickly reconstitute operations after an incident is paramount to reducing the length of the attack timeline and overall consequences to the Nation. There are two areas of concern that could inhibit the Sector's ability to reconstitute and then recover:

- The inability to recover due to unavailability of recovery capabilities; and
- The inability to recover due to exploitation of recovery capabilities.

There are several vulnerabilities that could cause both identified concerns, including lack of sustainable engineering; concentration of human and/or infrastructure resources to create engineering fixes; lack of sufficient infrastructure (e.g., bandwidth, geographically diverse servers) to distribute patches (good or bad ones); and the inability to communicate with vendors and/or consumers.

Two vulnerabilities, in particular, could cause the exploitation of recovery capabilities. These include reports containing false information on engineering fixes published by a trusted source and the exploitation (e.g., spoofing) of infrastructure to distribute patches. Both of these actions could cause incident managers to unknowingly provide ineffective recovery actions.

Economic consequences could be significant if the Sector is unable to quickly establish normal operations after an attack. For example, by disrupting the Sector's ability to distribute patches in a timely manner, an actor could cause lasting cross-sector economic consequences.

Impact to Mitigation and Prevention of Similar/Same Attack Occurrence

The inability to provide protection from future occurrences and/or recurrence of similar or same attacks is of particular concern. This capability is the backbone of the incident management lifecycle. Without this ability, it would be very difficult to maintain operations as lessons learned from previous successful attacks would not be incorporated into risk management efforts. There are three areas of concern:

- Lack of a defined process and mechanism to integrate lessons learned into product and service design and development;
- Lack of training or awareness programs to educate the public and private sector of likely future incidents; and
- Lack of preventive guidance, best practices, simulation, and testing based on lessons learned.

Failure to integrate lessons learned into future products and services and incident response procedures and policies marginalizes any benefits gained through past experiences. As such, if any of these three concerns were realized, it would greatly impact the Sector's ability to continuously improve prevention and protection activities and response and recovery capabilities learned and adapt from previous attacks. Because the integration of lessons learned into the IT Sector's operations fosters continuous learning and reinvigorates and improves prevention techniques, an impact to this mission could significantly hamper the IT Sector's risk management efforts.

***Providing Incident Management Capabilities* Relative Risk Table**

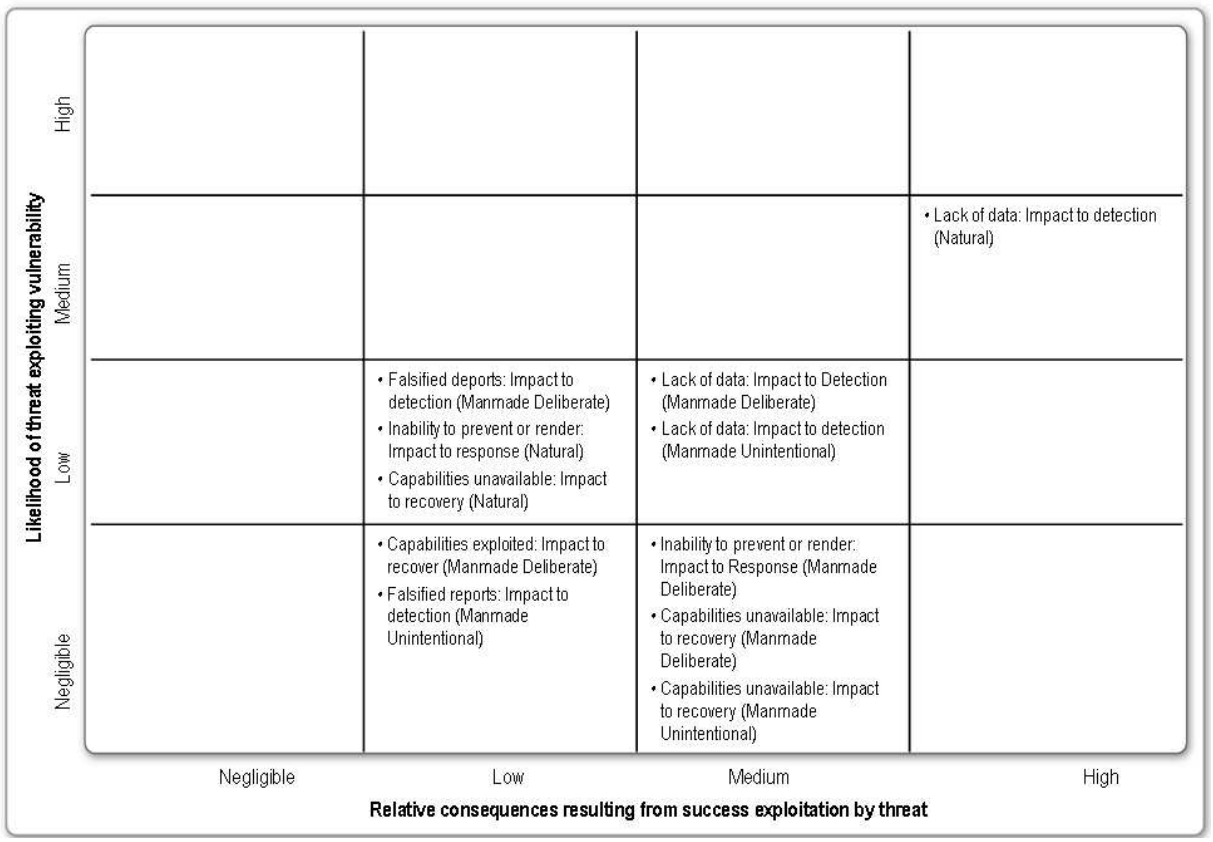


Figure 26: Relative Risks to the *Provide Incident Management Capabilities* Function

3.6.2 Mitigations

As part of the Baseline Risk Assessment, the SMEs identified existing and future mitigations that address the risks outlined for the *Provide Incident Management Capabilities* function. The mitigations were categorized as existing mitigations, mitigations currently being enhanced and improved, and future mitigations. These categories will assist the IT Sector outline R&D and protective program priorities

Existing Mitigations

- Organization-level incident response capabilities: Many organizations have in-house incident response capabilities that include expertise from other incident management service providers, each of which could collaborate with ISACs or other operations centers. This includes adequate staffing and training of all internal and external employees, as well as third-party vendors, to learn

and adapt from previous attacks as well as guidance, best practices, simulation, and testing to reinvigorate and improve prevention techniques.

- National-level incident response capabilities: Incidents that cause or could potentially cause consequences that are not limited to an organization are managed through national-level incident response capabilities. Entities that provide these capabilities regularly share technical and strategic threat and vulnerability information and mitigate overall risks to existing or potential incidents. Examples of national-level incident response capabilities include the United States Computer Emergency Readiness Team (US-CERT) and the IT-ISAC, as well as working groups that address cross-sector cyber infrastructure issues, including the Cyber Security Cross Sector Working Group and the ISAC Council. These mechanisms can also take the form of training or awareness programs to educate government and industry of likely future incidents.

- Infrastructure and workforce diversity: In addition to redundant infrastructure and continuous monitoring, detection, and response capabilities, the providers of these services have geographically dispersed workforces and resources.

- Information sharing enhancements: The Sector currently participates in numerous information sharing programs designed to create common situational awareness for owners and operators of critical IT functions, assets, systems, and networks. Broad sharing of information aids in ongoing risk management operations and benefits all aspects of the incident management lifecycle.

Mitigations Currently Being Enhanced and Improved

- Incident information sharing and situational awareness: The IT Sector has increasingly engaged with federal government partners to improve information sharing, specifically on cyber threat information. Several current information sharing programs (e.g., US-CERT) are being enhanced to better integrate the private sector into ongoing federal cybersecurity programs.

Potential Future Mitigations

- Continuous feedback and learning enhancements: Continuous feedback and learning enables incident response teams, procedures, and policies to benefit from the successes and shortcomings of previous incident response activities. The IT Sector should incorporate Sector-wide lessons learned into training and awareness materials for incident response teams and into incident response procedures and policies to promote continuous learning to improve future incident management capabilities.

- Alternative mechanisms for delivering patches: A protective program initiative is needed to provide mechanisms for delivering patches and other software to critical users if key Internet or network functions are not available. The IT Sector needs to develop an out-of-band data delivery capability that allows the Sector to respond and recover more effectively.

3.7. Dependencies and Interdependencies

3.7.1 Critical IT Sector Function Interdependencies

The critical IT Sector functions are highly interdependent. Each function supports the others, and these interdependencies highlight the need and reality of IT Sector entities' ongoing risk management efforts. Due to the interdependent nature of each function, SMEs conducted a separate dependency analysis of each function to explain how function-level risks can cause cascading impacts to other critical functions.

A cross-functional analysis of the IT Sector makes apparent the extent to which each function is dependent on the other functions, as well as identifying those functions most affected by cross-functional exploitations. Some functions are more specialized than others, and some have broader applications to operations in cyberspace and critical infrastructures. Some functions, such as *Produce and Provide IT Products and Services*, are so broad that practically any IT Sector operation has some kind of dependency. Other functions, such as *Provide Incident Management Capabilities*, are so temporally-specific that under normal operational conditions, no function may be dependent.

Figure 27 illustrates the cross-functional interdependencies of the critical functions and relationships across the functions. The table is not meant to be a comprehensive, detailed cross-functional analysis. Instead, the table's purpose is to indicate those functions that are dependent on other functions, and whether that dependency is High, Medium, Low, or Negligible.[51] The purpose of this ranking is to indicate areas of interdependency that may indicate key risk areas. The first order functions, or those that are exploited, are listed vertically down the y-axis. The cascading impacts to the other functions are listed horizontally across the x-axis.

- The production of IT products and services spans the entire IT Sector's infrastructure. Internet Routing provides a conduit upon which DNS operates.
- Identity management allows for secure Internet communication upon which the Internet Content function's operations are heavily dependent.
- Incident Management is needed to support ongoing risk management activities and is typically more independent than, but equally important as, the other critical functions.

[51] The ratings described in this section are not *risk* ratings associated with the IT Sector's risk assessment methodology. Instead, these ratings are intended to highlight the *dependencies and interdependencies* across the critical IT Sector functions.

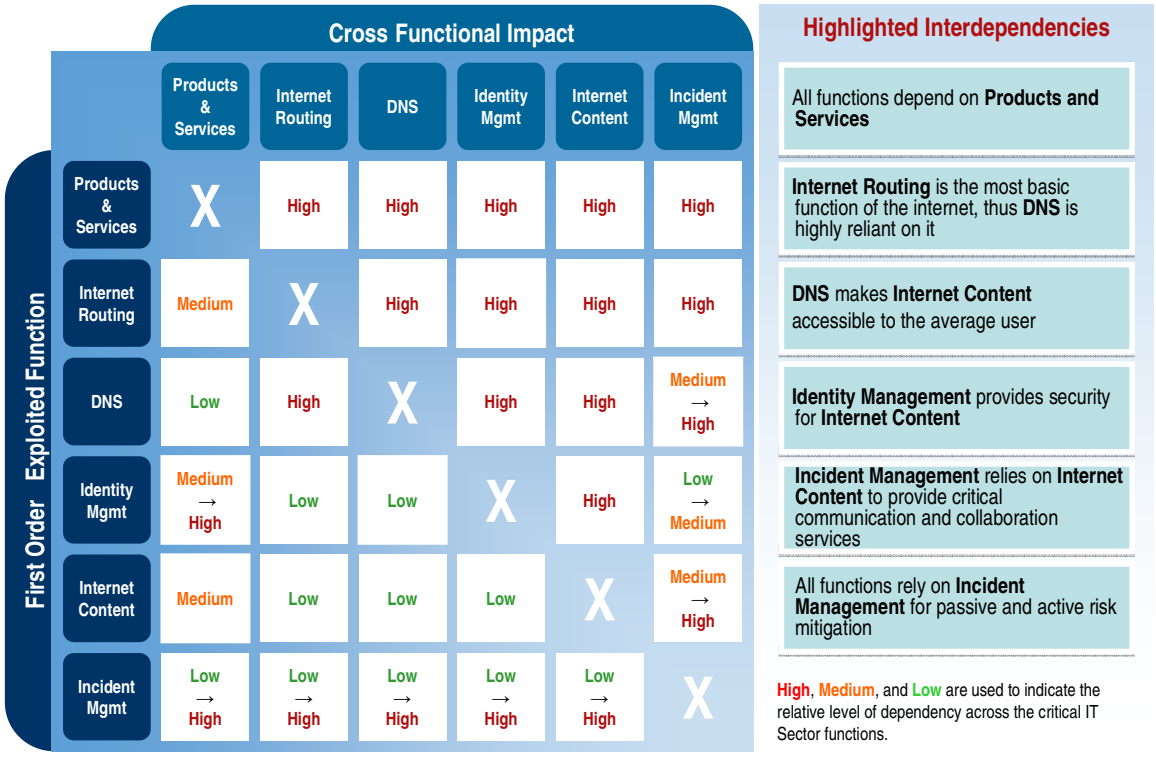


Figure 27: Cross-Functional Dependencies and Interdependencies

The cross-functional analysis reveals several key interdependencies that may be areas of heightened risk in the IT Sector. The areas discussed below were assigned a *High* interdependency in Figure 27. They are not the only ones that have been given a *High* interdependency ranking, but they are the dependencies that would have a significant impact on Sector operations and are illustrative of function interdependencies as a whole. Since there are no *Negligible* values assigned in Figure 27, no function is entirely independent of the other functions.

Exploited Function: Products and Services → Cross-Functional Impact: All Functions

As the broadest functional category, exploitation of, or an attack on, the Products and Services function could have the most wide-ranging effect on Sector operations. Interruptions in the supply chain for Internet hardware and software would affect the ability of ISPs to expand traffic capacity, as well as to maintain and upgrade firewalls, virus screening, and security services. Disruptions in wire line, fiber, microwave, and satellite communications services could cut off key long-haul, high-capacity Internet trunks. Other communications problems could isolate Internet users whose services depend on ISPs who depend on communications providers for their Internet connections.

Exploited Function: Internet Routing → Cross-Functional Impact: DNS

Internet Routing and DNS have a relatively greater interdependency between each other than other functions. The service each function provides enhances the other. In the event that the Internet routing function is impacted, DNS will not have data to resolve domain names and IP addresses, or the data could be resolved incorrectly or inaccurately.

Exploited Function: DNS → Cross-Functional Impact: Internet Content

Most Internet content would be unreachable if there were no DNS to resolve text URLs to numeric IP addresses. Content providers could circumvent a DNS outage by publishing the IP addresses for specific

sites or Web pages, but this is not an efficient method for name resolution. It would also reduce the flexibility Internet content providers have to move sites and content to different IP addresses for security or performance reasons. Content providers can use DNS to present the same Uniformed Resource Locator (URL) to Internet users even though the actual IP addresses may change.

Exploited Function: Identity Management → Cross-Functional Impact: Internet Content

The Internet Content function depends on the Identity Management function to provide for the security of its data. Internet content, such as financial records, personal data, credit card and Social Security numbers, and e-mail is protected by access codes or passwords. Large systems that consolidate this type of data, such as corporate personnel records and credit card files, are attractive targets for hackers and on-line thieves.

Exploited Function: Internet Content → Cross-Functional Impact: Incident Management

The Incident Management function relies on Internet Content to provide critical communications and collaboration tools needed to effectively respond to a cyber incident. If incident responders cannot communicate with key Sector owners and operators, it may significantly hamper efforts to patch affected assets, systems, or networks. Besides affecting response efforts, an exploitation of Internet Content could lead to ineffective prevention methods on the part of the Incident Management function. The Sector relies on publicly available threat and vulnerability data to guide prevention efforts. If this content was maliciously manipulated in some way, the Sector may be unable to effectively promote effective prevention processes.

Exploited Function: Incident Management → Cross-Functional Impact: All Functions

During normal Sector operations, the other functions operate relatively independent of the Incident Management function. While the Incident Management function provides for ongoing prevention and protection efforts, the other functions are not critically dependent on its operation. However, during times when an active exploitation of another function is taking place, the Incident Management function becomes critically important. For this reason, the cross-functional impact of an exploitation of the function was given a range of ratings (Low to High) as the current operating environment (passive monitoring versus active response) determines the function's criticality.

3.7.2 IT Sector Dependencies

The IT Sector depends upon several key utilities, services, and products provided by other critical infrastructure sectors. Sustained interruption of any one of these infrastructures due to events outside the control of the IT Sector can cause failures or disruptions in one or more critical IT Sector functions.

Millisecond Sectors

- **Communications Sector**: The IT and the Communications Sectors are inextricably linked and share many collocation facilities for switching and routing functions. The IT Sector depends on carrier cable networks and satellite communications for the delivery and distribution of critical functions. Although there is redundancy within telecommunications networks, a sustained local or regional outage could result in a denial-of-service.

- **Energy Sector**: The IT Sector, like all other sectors, is highly dependent on power from the electric grid for sustained operation of data centers, production facilities, carrier hotels, and other physical assets. Although most, if not all, critical IT facilities have alternative and/or redundant emergency power supplies in place, a sustained interruption of electrical power would inevitably cause a denial-of-service. Upstream dependencies include the Dams and Nuclear Sectors, which supply power to the electric grid.

Other Sectors

- **Banking and Finance Sector:** Access to safe and stable capital and financial markets provides the mechanism by which IT Sector entities can acquire raw materials, maintain workforces, and purchase services in support of their operations. Without the free-flow of capital throughout global markets, the products and services provided by the IT Sector would not be possible. In addition, global economic conditions directly influence the decisions made on a daily basis by IT Sector owners and operators. Decision-makers are influenced by market forces when they determine when, where, how much, and what type of goods are services will be purchased in support of their operations. A stable and reliable system to conduct financial transactions and save capital is required for many of the supply chain dependent processes of IT Sector entities to continue as well.

- **Chemical Sector**: The IT Sector depends on raw and synthetic materials in the production of hardware and software products. Consumers of IT Products and Services expect that these products are trustworthy and will operate reliably in their environment. The Chemical Sector provides an array of raw and synthetic materials for use in manufacturing these products and can be found in everything from Uninterruptible Power Supplies (UPS) to backlit liquid crystal display (LCD) panels and circuit boards to cable sheathing. Degradation of these materials can cause fires or corrosion; produce conditions for fungus growth; produce harmful fumes; or reduce the operating life of the equipment, thus causing a denial-of-service, damage to equipment, or injury to personnel.

- **Healthcare and Public Health Sector:** Providing the critical IT Sector functions depends on a productive, innovative, and highly-skilled workforce. The health and safety of the workforce is paramount in maintaining such a workforce. Therefore, the Healthcare and Public Health Sector plays an important role in protecting the workforce from disease and pandemics as well as promoting a healthy lifestyle so workers have limited absences due to illnesses, especially those that are preventable.

- **Transportation Sector**: The IT Sector is reliant on the Transportation Sector as part of its supply chain for producing and providing critical IT Products and Services, since components must be physically transported from one location to another. Supply chain interruptions could result in unreliable or untrustworthy delivery as well as impacts to the just-in-time-delivery practices common within IT Sector entities' operations.

- **Water Sector**: Data centers often use high-tonnage heating, ventilation, and air conditioning (HVAC) systems that require drinkable water to operate in order to keep their computer systems cool and production plants require purified potable water for the generation of steam for cogeneration of electricity and steam-driven processes. A sustained loss of water to a facility can cause equipment shutdown or failure, resulting in a denial-of-service.

- **Federal Government**: Private IT Sector partners depend on U.S. government satellites to provide mapping and geospatial data and imagery services. The U.S. government also supports the IT Sector in providing and operating specific root, top level, and lower level DNS. Since the U.S. government owns the global positioning system (GPS), they reserve the right to limit this service for a variety purposes, thus potentially impacting some commercially-available services.

4 Risk Management Considerations

The risks to each of the IT Sector functions have been characterized by *consequence* and *likelihood* in order to suggest priorities for managing and mitigating risks. For each function, the *consequence* and *likelihood* of the risks have been rated as Negligible, Low, Medium, or High. The risks for each function have been indicated in the Relative Risk tables included in each function's analysis. A *consequence* for a function could be Low, while its *likelihood* could be High. This would indicate that even though it may be very likely that the threat or risk might happen, the consequences might be minimal (or not as nationally significant) as determined by the risk assessment SMEs.

The following table highlights the IT Sector's high consequence risks. These risks were identified by SMEs in a collaborative and iterative process that consisted of attack tree development, risk evaluation, and final analysis. Throughout this process, SMEs employed the IT Sector's risk assessment methodology. The items captured in the *Risks of Concern* column of the table highlight the risks of greatest concern to the confidentiality, integrity, or availability of the critical function. The *Mitigations* column is a summary of the mitigations identified within the function's analysis section, which address the highlighted risks.

Critical IT Sector Function	Risks of Concern	Mitigations (Existing, Being Enhanced, or Potential Future)
Produce and Provide IT Products and Services	❑ Production or distribution of untrustworthy critical product/service through a successful manmade deliberate attack on a supply chain vulnerability *(Consequence: High; Likelihood: Low)*	❑ Supply chain resiliency though redundancy and process controls - *Existing Mitigation* ❑ Sourcing strategies (i.e., careful monitoring of the availability and quality of critical raw materials) - *Existing Mitigation* ❑ Product recall informed by situational awareness and timely response to compromised production - *Existing Mitigation*
Provide Domain Name Resolution Services	❑ Breakdown of a single interoperable Internet through a manmade attack, and resulting failure of governance policy *(Consequence: High; Likelihood: Medium)* ❑ Large scale manmade Denial-of-Service attack on the DNS infrastructure *(Consequence: High; Likelihood: Low)*	❑ Processes that enhance quality assurance and ensure continuous monitoring of Domain Name System (DNS) infrastructure - *Existing Mitigation* ❑ Provisioning and the use of Anycast - *Existing Mitigation* ❑ Infrastructure diversity and protection enhanced redundancy and resiliency - *Mitigation Being Enhanced*
Provide Internet-based Content, Information, and Communications Services	❑ Manmade unintentional incident caused in Internet content services result in a significant loss of e-Commerce capabilities (Consequence: High; Likelihood: Negligible)	❑ Policy and access controls - *Existing Mitigation* ❑ Security training for users and small businesses - *Mitigation Being Enhanced* ❑ Enhance rerouting capabilities of the Communications and IT Sectors - *Potential Future Mitigation*

Critical IT Sector Function	Risks of Concern	Mitigations (Existing, Being Enhanced, or Potential Future)
Provide Internet Routing, Access and Connection Services	❑ Partial or complete loss of routing capabilities through a manmade deliberate attack on the Internet routing infrastructure *(Consequence: High; Likelihood: Low)*	❑ Enhanced routers (i.e., increased speed, reliability, and capacity of routers and router software) - *Existing Mitigation* ❑ Responsiveness to increasing Internet traffic - *Mitigation Being Enhanced* ❑ Increase physical security of Network Access Points and Internet Exchange Points - *Mitigation Being Enhanced* ❑ Improved incident response including contingency planning, training, and investment to enable skilled technicians to monitor networks to identify and respond to anomalies, outage, or incident - *Mitigation Being Enhanced*
Provide Incident Management Capabilities	❑ Impact to detection capabilities due to lack of data availability resulting from a natural threat *(Consequence: High; Likelihood: Medium)*	❑ National-level incident response and coordination capabilities - *Existing Mitigation* ❑ Infrastructure and workforce diversity - *Existing Mitigation* ❑ Information sharing enhancements creating common situational awareness - *Existing Mitigation*

Figure 28: IT Sector Risks of Concern

In the process of conducting the IT Sector Baseline Risk Assessment, public and private IT Sector partners recognized that there were several areas for additional exploration that may have implications for the IT Sector's risk profile. These areas include:

- Identity management[52]: Although digital certificates have been recognized as secure and reliable identity credentialing tools, they impose costly and complex administrative burdens on organizations that use PKI certificates. The weakest link, which can lead to consequences throughout the function, is the issuance of secure original identity documents. Until these issues are alleviated, the high level of assurance that digital certificates provide will remain the exclusive province of organizations that have the resources to support them or that require the levels of assurance and non-repudiation that PKI can provide. Due to the need to address the security of original identity documents, the content associated with this function only highlights *potential* risks to the function; relative ratings or analyses are not provided. Instead, public and private IT Sector partners identified this as an area that requires additional study before determining the overall risk to this critical IT Sector function.

- Manmade unintentional threats: The knowledge and measurements of risks associated with manmade unintentional threats, such as accidents, is relatively less mature than those associated

[52] Provide Identity Management and Associated Trust Support Services is one of the six critical IT Sector functions. Unlike the five functions highlighted in the table above, risk to this function was not evaluated because public and private sector partners identified this as an area that requires additional study before threats, vulnerabilities, and consequences can be assessed. The IT Sector Baseline Risk Assessment does include issues that could be considered and evaluated further when assessing risk to this function.

with manmade deliberate threats. While the IT Sector's risk assessment methodology (see Appendix 3) does include an approach to assessing risks from manmade unintentional threats, risk assessment SMEs recommended that this be studied further.

- Natural threats and the impacts to the infrastructure: Due to increased resiliency across IT Sector entities' infrastructures, most risks associated with natural threats are contained to the immediate locale or region of the incident. Additional mitigations for these risks could reduce the potential for local or regional incidents to cascade and create national-level impacts.

- Feasibility of the establishment of a national-level testing and simulation capability: Government agencies and the private sector rely on the continued operation of the Internet and its associated functions, and public and private sector partners each have important and unique roles in securing this infrastructure. While the availability of the Internet has remained relatively constant, it is recommended that the feasibility of a potential national-level testing and simulation capability be considered. The purpose of such a program or programs would be to model upgrades and changes to the Internet infrastructure and to simulate the effects of those changes. Such a program would imply that there is also a collaborative body that would analyze and create guidance for proposed infrastructure changes, based on the results of tests or simulations.

- National-level cybersecurity awareness program: Most Internet users are aware that there are significant threats to Internet content and the Internet infrastructure, but they may not be sure what they can do about them. Internet service providers, DNS server operators, hardware and software vendors, identity credential providers, and network first responders are more attuned to the risks and threats their businesses face, and most take actions to secure their operations. The development of a comprehensive and nation-wide cybersecurity awareness, training, and education program could coordinate the risk mitigation efforts of product, content, and Internet service infrastructure providers with users in government, military, educational, and private sector organizations. Efforts such as National Cyber Security Awareness Month, could serve as a model to develop year-round coordinated outreach and awareness programs. The objective of these programs is to make sure that risk mitigation activities are applied consistently across the provider and user communities. Public and private sector partners should consider enhancing or supplementing these efforts.

- Cross-sector interdependency analysis: No one sector can undertake cross-sector interdependency risk mitigation efforts alone. Studying cyber interdependencies between sectors may reveal risks not being managed in the gray areas, where sector responsibilities cross into one another. Although there are ongoing efforts in this area through the Partnership for Critical Infrastructure Security and the Information Sharing and Analysis Centers, the federal government can provide much needed resources including funding and forums for public and private sectors to jointly conduct cyber interdependency analyses, share interdependency information, and address resulting areas of risk.

Consistent with its approach to date, the IT Sector will continue to mature its risk assessment and management approach and processes. Addressing the risks highlighted in this assessment will require the continued public and private sector collaboration that has facilitated the development of this assessment. Therefore, this assessment will continue to evolve and be revised as the Sector addresses these risks. In addition, the IT Sector encourages and welcomes the active participation of additional SMEs in the IT Sector's risk management efforts to continue the expansion and increase the understanding of Sector-wide risk.

Appendix 1—Acronyms

ARIN	American Registry for Internet Numbers
AS	Autonomous Systems
ASN	Autonomous System Number
BGP	Border Gateway Protocol
BIND	Berkeley Internet Name Domain
CA	Certificate Authority
CAC	Common Access Card
cc TLD	country code top level domain
CIKR	Critical Infrastructure and Key Resource
CMMI	Capability Maturity Model Integration
COOP	Continuity of Operations
DDoS	Distributed Denial of Service
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DoS	Denial-of-Service
GCC	Government Coordinating Council
gTLD	global Top Level Domain
Gbps	Gigabytes Per Second
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation, and Air Conditioning
IANA	Internet Assigned Numbers Authority
ID	identification
IdITF	Identity Issues Task Force (NSTAC)
IDN	Internationalized Domain Name
IETF	International Engineering Task Force

IM	Instant Messenger
IP	Internet Protocol
IPsec	Internet Protocol Secure
IPv6	Internet Protocol version 6
ISAC	Information Sharing and Analysis Center
ISIS	Intermediate System and Internet Security
ISP	Internet Service Providers
IT	Information Technology
IXP	Internet Exchange Points
LCD	Liquid Crystal Display
LSS	Lean Six Sigma
MD5	Message-Digest algorithm 5
MITM	Man-In-The-Middle
MRP	Material Requirements Planning
NANOG	North American Network Operators' Group
NAP	Network Access Points
NIPP	National Infrastructure Protection Plan
NSEP	National Security Emergency Preparedness
NSTAC	National Security Telecommunications Advisory Committee
OODA	Observe, Orient, Decide, and Act
OSPF	Open Shortest Path First
P2P	Peer-To-Peer
PC	Personal Computer
PCIS	Partnership for Critical Infrastructure Security
PIN	Personal Information Number
PIV	Personal Identity Verification

PKI	Public Key Infrastructure
POP	Point of Presence
RA	Registration Authority
R&D	Research and Development
RIPE	Réseaux IP Européens
RMA	Return Material Authorization
RPKI	Resource Public Key Infrastructure
S-BGP	Secure Border Gateway Protocol
SCADA	Supervisory Control and Data Acquisition
SCC	Sector Coordinating Council
SME	Subject Matter Expert
SQL	Structured Query Language
SSP	Sector-Specific Plan
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege
TLD	Top-Level Domain
UPS	Uninterruptible Power Supply
US-CERT	United States Computer Emergency Readiness Team
USG	United States Government
VoIP	Voice-over-Internet Protocol
WISR	World Infrastructure Security Report
XC	Interexchange Carrier

Appendix 2—Glossary

Access: The ability, right, or permission to approach, enter, communicate with the target to exploit a vulnerability to cause an incident. Access can also be granted via a proxy.

Actor: An individual, group, organization, or nation-state whose actions may cause an *incident*. Actors fall into two categories depending on their *intent*—hostile and non-hostile. Hostile actors intend to harm or inappropriately use critical IT Sector functions and sub-functions to cause an *incident*, and these actors conduct deliberate actions for that result. Non-hostile actors do not intend to inappropriately use critical IT Sector functions and sub-functions to cause an *incident*, but their action or inaction causes one.

Actor Autonomy: The autonomy by which the actor performs their daily duties.

Capabilities: The combination of *resources* and *access* of an actor to damage, disrupt, or destroy critical IT Sector functions.

Careless: Operating in a negligent manner with wanton or reckless disregard of policies, plans, and procedures.

Confidentiality: The unauthorized disclosure of information residing on information systems that support the critical sub-function.

Consequence: The effect of an event, incident, or occurrence. For the purposes of the IT Sector Baseline Risk Assessment, the expected range of direct and indirect impacts that can occur should a threat exploit vulnerabilities in a critical function.

First-order impacts: Consequences that directly affect the critical IT Sector function.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of critical IT Sector functions and sub-functions.

Intent: The purpose of an *actor's* operation (i.e., *strategic objective*) and the *tactical outcome* used to achieve that objective.

Likelihood of threat: The probability of an *incident* occurring. Many factors need to be considered in making this assessment ranging from the chance occurrence of a natural event to the deliberate or accidental act of an *actor*.

Limits: The legal and ethical codes and/or beliefs that may constrain an *actor*. When determining actor *limits*, the maximum or worst case scenario should be assumed.

Manmade Threat: *Incidents* that are either enabled by or caused by human beings, such as unintentional acts (e.g., inadvertent data entry) or deliberate actions.

Natural Threat: A non-manmade *incident* caused by biological, geological, seismic, hydrologic, or meteorological conditions or processes in the natural environment. The threat posed by natural events is dependant on the location, community infrastructure, and climate. Natural threats will be assessed using a different process than that being used to analyze manmade threats from various *actors*.

Policy Adherence: A determination of the attitude the actor has towards function/sub-function, corporate, organizational, or other policies.

Reckless: Operating in a negligent manner in willful or wanton disregard of policies, plans, and procedures.

Resources: The *sophistication*, *money, people* (including *skill level*), *time*, and *tools* that the *actor* uses to cause an *incident*.

Risk: The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.

Role in Function: Determine the role the actor plays within the function considering access to critical systems as well as the actors overall autonomy within the function.

Second-order impacts: Consequences that affect entities inside and outside the IT Sector that depend on the function or sub-function.

Skill level: The special training or expertise that the *actor* possesses and/or requires to cause an *incident*.

Sophistication: An *actor's* ability to align, structure, integrate, innovate, and develop the necessary means to cause an *incident*.

Strategic Objective: What the actor hopes to accomplish by causing an *incident* (i.e., motivation or "why"). In the case of an accident or unintentional *incident*, the strategic objective will be articulated as "No stated objective/unintentional."

Tactical Outcome: What the actor does or does not do to cause an incident.

Tactical Means: The specific action or inaction that enables the tactical outcome (i.e., how the tactical outcome is realized). These actions or inactions impact the target.

Target: The people, process, technology, or physical elements of critical IT Sector functions and/or sub-functions destroyed, incapacitated, or exploited to cause an *incident*.

Threat: The natural or manmade *incidents* (intentional or unintentional) that would be detrimental to the IT Sector.

Tools: The technology, materials, or instruments used to cause an *incident*.

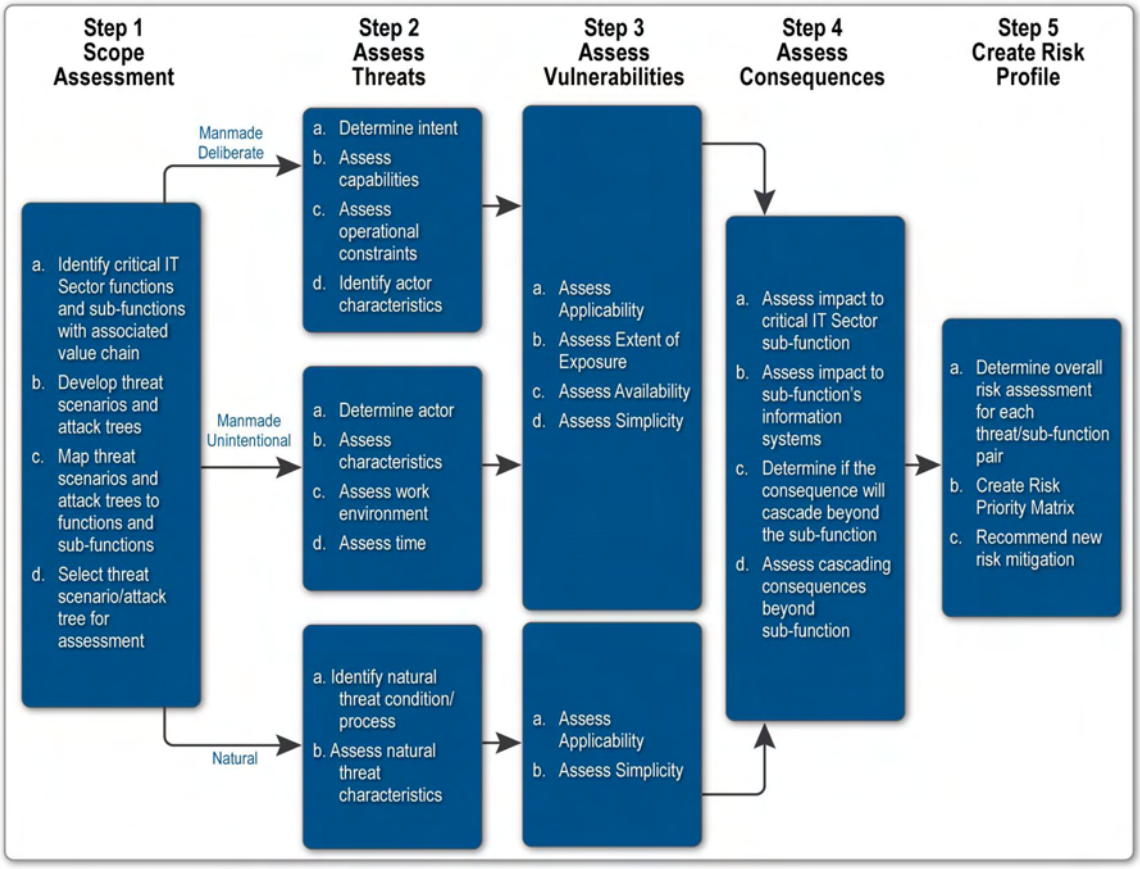
Visibility: The extent to which an *actor's* identity is hidden, either through their own actions or through other circumstances.

Vulnerability: A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard.

Work Environment Stress: A measure of the stress, both physical and psychological, placed upon the actor by their work environment.

Appendix 3—IT Sector Risk Assessment Methodology Details

As articulated in Section 2 of this report, the IT Sector's risk approach evaluates risk across the Sector by focusing on critical functions rather than specific organizations or assets. This appendix provides the detailed risk assessment approach that has been developed by the IT Sector. The methodology will be updated and revised as necessary.



IT Sector Risk Assessment Methodology – Manmade Deliberate				
Threat Framework				
	Threat Factor	**Criteria**	**Definition**	**Rating**
Determine Intent	Strategic objective	Power Projection	Demonstrate elements of national power (political, economic, informational, or military)	
		Political Pressure	Exert influence over governmental operation	
		Obstruction	Cause a delay in the conduct of business	
		Deception	Mislead	
		Intelligence Gathering	Collect intelligence on other entities	
		Counterintelligence	Gather information and conduct activities to protect against espionage or other intelligence activities	
		Financial/Technical Gain	Increase monetary resources or technological capabilities	
		Amusement	Perform for enjoyment	
		Gratuitous Defacement or Damage	Disfigure or impair the usefulness	
		Advocacy	Plead or argue in favor of a cause, idea, or policy	
	Intended outcome	Acquisition/Theft	Wrongfully take personal goods or property of another	
		Damage	Impair the usefulness of	

IT Sector Risk Assessment Methodology – Manmade Deliberate Threat Framework				
	Threat Factor	**Criteria**	**Definition**	**Rating**
		Embarrassment	Create difficulties for organization/government by making inadequacies public	
		Gratuitous Defacement	Disfigure	
Assess Capabilities	Resources – Sophistication	Government	Controls public assets and functions within a jurisdiction; very well resourced. Entity persists long-term	High
		Organization	Private, but larger and better resourced than Team; typically a company or similar structure. Usually with multiple geographies. Entity persists long-term	High
		Team	Formal organization with a leader, typically more motivated and organized around an objective. Typically only one geography. Entity persists long-term	Medium
		Contest	Short-lived and perhaps anonymous interaction that concludes when single objective is complete	Low
		Club	Members interact on a social and volunteer basis and often have little personal interest towards a specific target; for example, a group of teenagers looking for any car easily stolen for simple joyriding. Group persists long-term.	Low
		Individual	Average person who acts independently	Negligible
	Resources – People (Skills)	Adept	Expert in technology, tools, and methods and can both apply existing and create new attacks methodologies to greatest advantage	High
		Operational	Understands underlying technology, tools, or methods and can create new attacks within a narrow domain	Medium
		Minimal	Can copy and use existing techniques	Low
		None	Average intelligence and ability and can easily carry out random acts of violence, disruption, or destruction, but has no expertise or training in specific methods necessary for an incident	Negligible
	Resources – Tools	Tools required, not readily available (i.e., actor needs to develop)	N/A	High
		Tools required, readily available, and difficult to adapt	N/A	Medium
		Tools required, readily available, and easily adaptable	N/A	Low
		No tools required	N/A	Negligible
	Resources – Money	Unlimited funding	Greater than $5,000,000	High
		Significant funding	$500,000 - $5,000,000	Medium
		Limited funding	$5,000 - $500,000	Low
		No funding	Less than $5,000	Negligible
	Resources – Time	Unlimited time	Greater than 5 years	High
		Significant time	1-5 years	Medium
		Limited time	Less than 1 year (not real-time)	Low
		No time	Real-time	Negligible
	Access – Physical	Insider (authorized)	Actor permanently has the credentials to gain physical access (e.g., company employees)	High
		Outsider (authorized)	Actor does not permanently have the credentials to gain physical access, but they gain that access through legitimate means at a specific time (e.g., maintenance worker or any visitor processed through security)	High

IT Sector Risk Assessment Methodology – Manmade Deliberate Threat Framework				
	Threat Factor	Criteria	Definition	Rating
		Insider (proxy)	Actor does not have the credentials to gain physical access, but uses an authorized insider to gain access to the target (e.g., insider is used/coerced to conduct the attack)	Medium
		Outsider (proxy)	Actor does not have the credentials to gain physical access, but uses an authorized outsider to gain access to the target (e.g., sympathetic 3rd party vendor is used/coerced to conduct the attack)	Medium
		Insider (unauthorized)	Actor has the credentials to gain physical access to some aspect of the function/function, but not the target (e.g., company employee that goes to an area of facility/cyber system where he or she is not allowed)	Low
		Outsider (unauthorized)	Actor does not have the credentials to gain physical access (e.g., breaking and entering)	Low
		No access	Actor does not require physical access to target	Negligible
	Access – Logical	Insider (authorized)	Actor permanently has the credentials to gain logical access (e.g., company employees)	High
		Outsider (authorized)	Actor does not permanently have the credentials to gain logical access, but they gain that access through legitimate means at a specific time (e.g., maintenance worker or any visitor processed through security)	High
		Insider (proxy)	Actor does not have the credentials to gain logical access, but uses an authorized insider to gain access to the target (e.g., insider is used/coerced to conduct the attack)	Medium
		Outsider (proxy)	Actor does not have the credentials to gain logical access, but uses an authorized outsider to gain access to the target (e.g., sympathetic 3rd party vendor is used/coerced to conduct the attack)	Medium
		Insider (unauthorized)	Actor has the credentials to gain logical access to some aspect of the function/function, but not the target (e.g., company employee that goes to an area of facility/cyber system where he or she is not allowed)	Low
		Outsider (unauthorized)	Actor does not have the credentials to gain logical access (e.g., breaking and entering)	Low
		No access	Actor does not require logical access to target	Negligible
	Tactical Means	Copy	A replica of the people, process, technology, or physical elements of critical IT Sector functions and/or functions is made, giving both the sector and the actor simultaneous access to the function	
		Deny	Leveraging their own influence to impact or affect the sector's desire to move forward or use people, processes, technologies, or physical elements of critical IT Sector functions and/or functions	
		Destroy (includes death)	The people, process, technology, or physical elements of critical IT Sector functions and/or functions are completely and permanently destroyed and of no utility or value to either the sector or the actor	
		Degrade/Injure	The people, process, technology, or physical elements of critical IT Sector functions and/or functions are damaged, but are still in the sector's possession providing only limited functionality or value	
		Take	The actor has possession of people, process, technology, or physical elements of critical IT Sector functions and/or functions and the sector has no access to them	
		Does Not Care	The actor does not have a rational plan, or, may make a choice to opportunistically cause an incident	

IT Sector Risk Assessment Methodology – Manmade Deliberate Threat Framework				
	Threat Factor	**Criteria**	**Definition**	**Rating**
		Exploit	Cause the people, process, technology, or physical elements of critical IT Sector functions and/or functions to perform something they were not intended to do	
Assess Operational Constraints	Visibility	Overt	The actor's identity and attack (or intent to attack) intentionally become obvious before or at the time of execution	
		Does Not Care	The actor does not have a rational plan, may make a choice opportunistically at the time of attack, or may not place importance on secrecy	
		Unknown	It is unknown if the actor will keep their identity and/or actions hidden	
		Covert	The attack is known at or shortly after the fact, but the identity of the actor remains unknown	
		Clandestine	Neither the attack nor the actor are discovered	
	Limits	None	No adherence to moral codes	High
		Unknown	It is unknown if there are limits that could impact the potential for causing an incident	High
		Illegal, major	No account is taken of the law; felonious behavior up to and including significant financial impact and extreme violence	Medium
		Illegal, minor	Relatively minor, non-violent transgressions of law can occur, such as vandalism or trespass	Medium
		Legal	Actors typically act up to the limits but remain within the letter and intent of applicable laws	Low
		Code of Conduct	An ethical code of conduct is generally accepted for a profession or exchange, and actors typically follow it	Low
Identify Actor Characteristics	Hostile Actors	Anarchist	Someone who rejects all forms of structure, private or public, and acts with few constraints	
		Corporate Spy	Professional data gatherer as a trusted insider, generally with a simple profit motive	
		Corrupt Government Official	Person who inappropriately uses his or her position within the government to acquire function resources	
		Cyber Vandal	Derives thrills from intrusion or destruction of property, without agenda	
		Data Miner	Professional data gatherer external to the company (includes cyber methods)	
		Employee, Disgruntled	Current or former employee with intent to harm the function	
		Foreign Government Agent/Spy	State-sponsored spy or agent as a trusted insider, supporting idealistic goals	
		Foreign Military	Foreign entity that attacks the United States and/or its allies because of disagreement with or dislike of the United States and/or its allies	
		Government Cyberwarrior	State-sponsored attacker with significant resources to affect major disruption on national scale	
		Irrational Individual	Someone with illogical purpose and irrational behavior	
		Mobster	Manager of organized crime organization with significant resources	
		Radical Activist	Highly motivated, potentially destructive supporter of cause	
		Terrorist	Person who relies on the use of violence to support personal socio-political agenda	
		Thief	Opportunistic individual with simple profit motive	
		Nation-state	A sovereign territory with significant resources to cause harm	
		Other	All other actors	

IT Sector Risk Assessment Methodology – Manmade Deliberate Vulnerability Framework				
	Vulnerability Factors	**Definition**	**Criteria**	**Rating**
Assess Applicability of Vulnerabilities	People Process Technology Physical Other	How well do vulnerability(-ies) align with threat requirements (based on a threat's intent, capabilities, and/or operational constraints)?	Vulnerability(-ies) are well aligned with the threat requirements and can easily be exploited	High
			Vulnerability(-ies) are not optimal for the threat, but can be adapted for use with some effort	Medium
			Vulnerability(-ies) are not well suited to the threat requirements, but can be used if they are the only opening	Low
			Vulnerability(-ies) are essentially useless to the threat	Negligible
Assess Extent of Exposure of Vulnerabilities	People Process Technology Physical Other	How discoverable and identifiable are vulnerability(-ies)?	Vulnerability(-ies) are easy to discover and identify	High
			Vulnerability(-ies) are easy to discover, but difficult to identify	Medium
			Vulnerability(-ies) are difficult to discover and identify	Low
			There is very limited potential of discovering and identifying vulnerability(-ies)	Negligible
Assess Availability of Vulnerabilities	People Process Technology Physical Other	At what frequency and length of time are vulnerability(-ies) accessible?	Vulnerability(-ies) are openly accessible at all times	High
			Vulnerability(-ies) are accessible at specific times for long durations	Medium
			Vulnerability(-ies) are accessible at specific times for short durations	Low
			Vulnerability(-ies) are restricted at all times, and are nearly inaccessible	Negligible
Assess Simplicity of Vulnerabilities	People Process Technology Physical Other	How easily can vulnerability(-ies) be exploited?	Very simple, vulnerability(-ies) can be exploited with limited resources	High
			Some general training or modest resources would be needed to exploit vulnerability(-ies)	Medium
			Specialized training or resources are needed to exploit the vulnerability(-ies)	Low
			Exploiting vulnerability(-ies) is complex and requires extensive training and significant resources	Negligible

IT Sector Risk Assessment Methodology – Manmade Deliberate Consequence Framework				
	Consequence Factor	**Criteria**	**Definition**	**Rating**
Assess Impact to Critical IT Sector Function	First Order Consequences	Confidentiality	The unauthorized disclosure of information residing on information systems that support the critical function	
		Integrity	The unauthorized modification or destruction of the function	
		Availability	The disruption of access to or use of the function	
Assess Impact to Critical IT Sector Function's Information Systems	First Order Consequences	Spoofing	The assumption of other user accounts, or the attributes of another user	

IT Sector Risk Assessment Methodology – Manmade Deliberate				
Consequence Framework				
	Consequence Factor	**Criteria**	**Definition**	**Rating**
		Tampering	The unauthorized alteration of data and system resources in inappropriate ways or by the inappropriate people	
		Repudiation	The dishonest denial of actions performed	
		Information Disclosure	The unauthorized access of data	
		Denial of Service	The inaccessibility of systems that perform acceptably when needed	
		Elevation of Privilege	The unauthorized increase of user privileges	
Determine if the Consequence will Cascade Beyond the Function	Time required to detect the incident	Predictive	The threat will be identified before the incident occurring	
		Real-time	N/A	
		Minutes	N/A	
		Hours	N/A	
		Days	N/A	
		Months	N/A	
	Time required to recover the function	Real-time	Accounts for mitigations that anticipate and preclude consequences	
		Minutes	Accounts for mitigations due to redundancy that enable continued real time services	
		Hours	Accounts for mitigations due to backup and redundancy	
		Days	Accounts for mitigations due to Continuity of Operations (COOP) Planning	
		Months	Accounts for mitigations due to other contingency planning efforts	
	Time required to reconstitute the function	N/A	Reconstitution of the function will not occur	
		Real-time	Accounts for mitigations that anticipate and preclude consequences	
		Minutes	Accounts for mitigations due to redundancy that enable continued real time services	
		Hours	Accounts for mitigations due to backup and redundancy	
		Days	Accounts for mitigations due to Continuity of Operations (COOP) Planning	
		Months	Accounts for mitigations due to other contingency planning efforts	
	Time to recover from the incident	Real-time	N/A	
		Minutes	N/A	
		Hours	N/A	
		Days	N/A	
		Months	N/A	
Assess Cascading	Executive (Federal)	Foreign policy	Mission is severely degraded	High

IT Sector Risk Assessment Methodology – Manmade Deliberate				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
Consequences Beyond Function - Government Essential Functions			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		National security/Defense	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Homeland security	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Revenue collection and spending	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Legislative (Federal)	Regulating taxing	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Regulating spending	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Grant necessary powers/funding for executive orders	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Judicial (Federal)	Court system	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	State/Local	Education	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Medicaid	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Economic Security	18 CIKR sectors	Agriculture and Food	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low

IT Sector Risk Assessment Methodology – Manmade Deliberate				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			No identifiable effect on mission	Negligible
		Banking and Finance	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Chemical	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Commercial Facilities	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Commercial Nuclear Reactors, Materials and Waste	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Communications	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Critical Manufacturing	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Dams	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Defense Industrial Base	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Drinking Water and Water Treatment Systems	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Emergency Services	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Energy	Mission is severely degraded	High

IT Sector Risk Assessment Methodology – Manmade Deliberate				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Government Facilities	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Information Technology	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		National Monuments and Icons	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Postal and Shipping	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Public Health and Healthcare	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Transportation Systems	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Public Health and Safety Missions	Emergency service missions	Emergency management (E911)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Fire, search, and rescue	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Law enforcement	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Emergency medical services	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low

IT Sector Risk Assessment Methodology – Manmade Deliberate				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			No identifiable effect on mission	Negligible
	Non-emergency service missions	Welfare needs (e.g., shelter, food, and water)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Medical incident management/containment	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Energy	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Communications	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Public Confidence Missions	Public confidence	Communication between the government and the public	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Confidence in corporate entities (measured by public awareness of corporate entities involved)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Confidence in government and economy (measured by public awareness of impact)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Corporate and government confidence and ability to continue investing in new and evolving technologies	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Threat Framework				
	Threat Factor	Criteria	Description	Rating
Determine Actor	Identify Actor	Employee	An individual employee	
		Team/Group	More than one employee	
		Division/Agency/ Organization	A population set within the function	
		Individual -Vendor/Contractor	Individual in a third-party business relationship with entity within function	
		Team/Group - Vendor/Contractor	Team/group in a third-party business relationship with entity within function	

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Threat Framework				
	Threat Factor	Criteria	Description	Rating
		Other	N/A	
	Role in Value Chain	Requirements, Design, R&D, Discovery	N/A	
		Implementation, Production, Manufacturing	N/A	
		Verify, Test, Validate, Pilot	N/A	
		Deliver, Deploy, Distribute	N/A	
		Sustain, Support, Respond, Update	N/A	
		Marketing and Sales	N/A	
		Training	N/A	
		Security and Quality Assurance	N/A	
		Not in Value Chain	N/A	
	Identify Cause	Untrained	Not adequately trained for role	
		Careless	Operating in a negligent or distracted manner with regards to policies, plans, and procedures	
		Reckless	Operating in a negligent manner in willful disregard of policies, plans, and procedures	
		Technical Flaw	Systemic flaw – not user-attributable	
		Other	N/A	
Assess Characteristics	Importance of Role	Key role in value chain	N/A	High
		Major role in value chain	N/A	Medium
		Minor role in value chain	N/A	Low
		No role in value chain	N/A	Negligible
	Access (Physical)	Insider (authorized)	Actor permanently has the credentials to gain physical access (e.g., company employees)	High
		Outsider (authorized)	Actor does not permanently have the credentials to gain physical access, but they gain that access through legitimate means at a specific time (e.g., maintenance worker or any visitor processed through security)	Medium
		Insider (unauthorized)	Actor has the credentials to gain physical access to some aspect of the function, but not the target (e.g., company employee that goes to an area of facility/cyber system where he or she is not allowed)	Low
		Outsider (unauthorized)	Actor does not have the credentials to gain physical access	Low
		No access	Actor does not require physical access to target	Negligible
	Access (Logical)	Insider (authorized)	Actor permanently has the credentials to gain logical access (e.g., company employees)	High
		Outsider (authorized)	Actor does not permanently have the credentials to gain logical access, but they gain that access through legitimate means at a specific time (e.g., maintenance worker or any visitor processed through security)	Medium
		Insider (unauthorized)	Actor has the credentials to gain logical access to some aspect of the function, but not the target (e.g., company employee that goes to an area of facility/cyber system where he or she is not allowed)	Low
		Outsider (unauthorized)	Actor does not have the credentials to gain logical access	Low
		No access	Actor does not require logical access to target	Negligible
	Skills	None	No level of skill, know-how, and abilities within the function	High

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Threat Framework				
	Threat Factor	Criteria	Description	Rating
		Minimal	Limited level of skill, know-how, and abilities within the function	Medium
		Operational	Significant level of skill, know-how, and abilities within the function	Low
		Adept	Expert level of skill, know-how, and abilities within the function	Negligible
		Not Applicable	Skills have no impact on accident occurring	Not Rated
	Tools	No tool required	No tool is necessary for the accident to occur	High
		Defective, misaligned, or uncalibrated tool	Tool required for accident to occur is defective, misaligned, or uncalibrated in some way as to create an accident	Medium
		Tool required	Tool required for the accident to occur	Low
	Policy Adherence	Unacceptable	Actor operates at standards well below the level of their position and requires remedial action	High
		Below expectations	Actor operates at standards lower than their position requires	Medium
		Meets expectations	Actor operates at the standards require for their position	Low
		Exceeds expectations	Actor clearly operates above the standards required for their position	Negligible
Assess Environment	Autonomy	No autonomy	Actor relies on many other people or a team before taking action	
		Limited autonomy	Actor relies on several other people before taking action	
		Significant autonomy	Actor relies on few people before taking action	
		Full autonomy	Actor relies on no other person before taking action	
	Workplace Stress	Extreme stress	Actor has extreme physical and psychological stress in their work or significant stresses in their work for long durations	High
		Significant stress	Actor has significant physical and psychological stress in their work for short durations	Medium
		Limited stress	Actor has limited physical and psychological stress in their work	Low
		Little to no stress	Actor has little physical and psychological stress in their work	Negligible
Assess Time	Time	Accident occurs without lead time (i.e., real-time)	Accident occurs and impacts the function instantly	High
		Accident occurs after limited lead time	Accident is developed and impacts the function after some time has passed	Medium
		Accident occurs only after lengthy lead time	Accident is developed and impacts the function after significant time has passed	Low

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Vulnerability Framework				
	Vulnerability Factors	Definition	Criteria	Rating
Assess Applicability of Vulnerabilities	People Process Technology Physical Other	How well do vulnerability(-ies) align with threat requirements (based on a threat's intent, capabilities, and/or operational constraints)?	Vulnerability(-ies) are well aligned with the threat requirements and can easily be exploited	High
			Vulnerability(-ies) are not optimal for the threat, but can be adapted for use with some effort	Medium

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Vulnerability Framework				
	Vulnerability Factors	**Definition**	**Criteria**	**Rating**
			Vulnerability(-ies) are not well suited to the threat requirements, but can be used if they are the only opening	Low
			Vulnerability(-ies) are essentially useless to the threat	Negligible
Assess Extent of Exposure of Vulnerabilities	People Process Technology Physical Other	How discoverable and identifiable are vulnerability(-ies)?	Vulnerability(-ies) are easy to discover and identify	High
			Vulnerability(-ies) are easy to discover, but difficult to identify	Medium
			Vulnerability(-ies) are difficult to discover and identify	Low
			There is very limited potential of discovering and identifying vulnerability(-ies)	Negligible
Assess Availability of Vulnerabilities	People Process Technology Physical Other	At what frequency and length of time are vulnerability(-ies) accessible?	Vulnerability(-ies) are openly accessible at all times	High
			Vulnerability(-ies) are accessible at specific times for long durations	Medium
			Vulnerability(-ies) are accessible at specific times for short durations	Low
			Vulnerability(-ies) are restricted at all times, and are nearly inaccessible	Negligible
Assess Simplicity of Vulnerabilities	People Process Technology Physical Other	How easily can vulnerability(-ies) be exploited?	Very simple, vulnerability(-ies) can be exploited with limited resources	High
			Some general training or modest resources would be needed to exploit vulnerability(-ies)	Medium
			Specialized training or resources are needed to exploit the vulnerability(-ies)	Low
			Exploiting vulnerability(-ies) is complex and requires extensive training and significant resources	Negligible

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Consequence Framework				
	Consequence Factor	**Criteria**	**Definition**	**Rating**
Assess Impact to Critical IT Sector Function	Confidentiality, Integrity, and Availability	Confidentiality	The unauthorized disclosure of information residing on information systems that support the critical function	
		Integrity	The unauthorized modification or destruction of the function	
		Availability	The disruption of access to or use of the function	
Assess Impact to Function's Information Systems	STRIDE	Spoofing	The assumption of other user accounts, or the attributes of another user	
		Tampering	The unauthorized alteration of data and system resources in inappropriate ways or by the inappropriate people	
		Repudiation	The dishonest denial of actions performed	

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
		Information Disclosure	The unauthorized access of data	
		Denial of Service	The inaccessibility of systems that perform acceptably when needed	
		Elevation of Privilege	The unauthorized increase of user privileges	
Determine if the Consequence will Cascade Beyond the Function	Time required to detect the incident	Predictive	The threat will be identified before the incident occurring	
		Real-time	N/A	
		Minutes	N/A	
		Hours	N/A	
		Days	N/A	
		Months	N/A	
	Time required to recover the function	Real-time	Accounts for mitigations that anticipate and preclude consequences	
		Minutes	Accounts for mitigations due to redundancy that enable continued real time services	
		Hours	Accounts for mitigations due to backup and redundancy	
		Days	Accounts for mitigations due to Continuity of Operations (COOP) Planning	
		Months	Accounts for mitigations due to other contingency planning efforts	
	Time required to reconstitute the function	N/A	Reconstitution of the function will not occur	
		Real-time	Accounts for mitigations that anticipate and preclude consequences	
		Minutes	Accounts for mitigations due to redundancy that enable continued real time services	
		Hours	Accounts for mitigations due to backup and redundancy	
		Days	Accounts for mitigations due to Continuity of Operations (COOP) Planning	
		Months	Accounts for mitigations due to other contingency planning efforts	
	Time to recover from the incident	Real-time	N/A	
		Minutes	N/A	
		Hours	N/A	
		Days	N/A	
		Months	N/A	
Assess Cascading Consequences Beyond Function - Government Essential Functions	Executive (Federal)	Foreign policy	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		National security/Defense	Mission is severely degraded	High

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Homeland security	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Revenue collection and spending	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Legislative (Federal)	Regulating taxing	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Regulating spending	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Grant necessary powers/funding for executive orders	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Judicial (Federal)	Court system	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	State/Local	Education	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Medicaid	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Economic Security	18 CIKR sectors	Agriculture and Food	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Banking and Finance	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			No identifiable effect on mission	Negligible
		Chemical	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Commercial Facilities	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Commercial Nuclear Reactors, Materials and Waste	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Communications	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Critical Manufacturing	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Dams	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Defense Industrial Base	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Drinking Water and Water Treatment Systems	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Emergency Services	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Energy	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Government Facilities	Mission is severely degraded	High
			Some mission degradation will occur	Medium

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Information Technology	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		National Monuments and Icons	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Postal and Shipping	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Public Health and Healthcare	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Transportation Systems	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Public Health and Safety Missions	Emergency service missions	Emergency management (E911)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Fire, search, and rescue	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Law enforcement	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Emergency medical services	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Non-emergency service missions	Welfare needs (e.g., shelter, food, and water)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Medical incident	Mission is severely degraded	High

IT Sector Risk Assessment Methodology – Manmade Unintentional				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
		management/containment	Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Energy	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Communications	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Public Confidence Missions	Public confidence	Communication between the government and the public	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Confidence in corporate entities (measured by public awareness of corporate entities involved)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Confidence in government and economy (measured by public awareness of impact)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Corporate and government confidence and ability to continue investing in new and evolving technologies	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible

IT Sector Risk Assessment Methodology – Natural						
Threat Framework						
	Threat Category	Threat Criteria	Severity Scale	Criteria	Definition	Rating
Identify Hazard Condition/ Process	Biological	Pandemic	Pandemic Severity Index (CDC)	Category 4/5	Case fatality ratio of over 1%	High
				Category 3	Case fatality ratio between 0.5% and 1%	Medium
				Category 2	Case fatality ratio between 0.1% and 0.5%	Low
				Category 1	Case fatality ratio less than 0.1%	Negligible
		Epidemic	Pandemic Severity Index (CDC)	Category 4/5	Case fatality ratio of over 1%	High
				Category 3	Case fatality ratio between 0.5% and 1%	Medium
				Category 2	Case fatality ratio between 0.1% and 0.5%	Low

IT Sector Risk Assessment Methodology – Natural						
Threat Framework						
	Threat Category	Threat Criteria	Severity Scale	Criteria	Definition	Rating
				Category 1	Case fatality ratio less than 0.1%	Negligible
	Geological & Seismic	Landslide	Landslide Velocity Scale (Varnes & Cruden)	Rapid to extremely rapid	Escape evacuation possible; structures; possessions, and equipment destroyed (> 1.8 m/hr)	High
				Moderate	Roads and strong buildings can be repaired temporarily during the movement (> 13 m/month)	Medium
				Slow	Some damaged buildings can be repaired during the movement (> 1.6 m/yr)	Low
				Very slow	Buildings and roads have only minor damage (≤ 1.6 m/yr)	Negligible
		Volcano	Volcanic Explosivity Index (USGS)	Cataclysmic	Plume reaching 10-25 km, and over 0.1 km3 of ejected volcanic material	High
				Severe	Plume reaching 3-15 km, and over 10,000,000 m3 of ejected volcanic material	Medium
				Explosive	Plume reaching 1-5 km, and over 1,000,000 m3 of ejected volcanic material	Low
				Gentle	Plume reaching less than 1 km, and less than 10,000 m3 of ejected volcanic material	Negligible
		Avalanche	Avalanche Destructive Force (USDA-US Forest Service)	Rapid to extremely rapid	Could destroy a railway car, large truck, several buildings, or a substantial amount of forest (mass of > 10,000 tons, > 2000 meter path length)	High
				Moderate	Could bury and destroy a car, damage a truck, destroy a wood frame house, or break a few trees (mass of > 1000 tons, > 1000 meter path length)	Medium
				Slow	Could bury, injure, or kill a person (mass of > 100 tons, > 100 meter path length)	Low
				Very slow	Relatively harmless to people (mass of < 100 tons, < 100 meter path length)	Negligible
		Earthquake	Richter Scale (USGS)	Major to Great	Can cause serious damage over larger areas (≥ 7.0 magnitude)	High

IT Sector Risk Assessment Methodology – Natural Threat Framework						
	Threat Category	Threat Criteria	Severity Scale	Criteria	Definition	Rating
				Moderate to Strong	Can cause major damage to poorly constructed buildings over small regions. At most slight damage to well-designed buildings (5.0 – 6.9 magnitude)	Medium
				Light	Noticeable shaking of indoor items, rattling noises. Significant damage unlikely (4.0 – 4.9 magnitude)	Low
				Micro to Minor	Often felt, but rarely causes damage (≤ 3.9 magnitude)	Negligible
	Hydrologic & Meteorological	Drought	Palmer Drought Severity Index (NOAA-Drought Information Center)	Extreme to exceptional drought	Major crop/pasture losses; widespread water shortages or restrictions (PDSI < -4)	High
				Severe drought	Crop or pasture losses likely; water shortages common; water restrictions imposed (PDSI -3 to -3.99)	Medium
				Moderate drought	Some damage to crops, pastures; streams, reservoirs, or wells low, some water shortages developing or imminent; voluntary water-use restrictions requested (PDSI -2 to -2.99)	Low
				Abnormally Dry	Going into drought: short-term dryness slowing planting, growth of crops or pastures. Coming out of drought: some lingering water deficits; pastures or crops not fully recovered (PDSI > -1.99)	Negligible
		Flood	Flood Severity Categories (NOAA-National Weather Service)	Record flooding	Flooding that equals or exceeds the highest stage or discharge at a given site during the period of record keeping	High
				Major flooding	Extensive inundation of structures and roads. Significant evacuations of people and/or transfer of property to higher elevations	Medium
				Moderate flooding	Some inundation of structures and roads near stream. Some evacuations of people and/or transfer of property to higher elevations are necessary	Low

IT Sector Risk Assessment Methodology – Natural Threat Framework						
	Threat Category	Threat Criteria	Severity Scale	Criteria	Definition	Rating
				Minor flooding	Minimal or no property damage, but possibly some public threat or inconvenience	Negligible
		Tsunami	Tsunami Intensity Scale (Papadopoulos-Imamura)	Destructive	Vessels washed away or onshore. Flooding damages buildings and causes panic	High
				Damaging	Extensive flooding, violent oscillating of vessels, and damage to buildings	Medium
				Strong	Felt onboard vessels; may cause crashing of small vessels and flooding of near-shore structures	Low
				Not felt	No damage, but may be observed by vessels and people on the coasts	Negligible
		Winter Storm	Northeast Snowfall Impact Scale (NOAA-National Weather Service)	Category 4/5	Crippling to extreme – huge areas of 10-in. (25-cm) snowfalls, and each case is marked by large areas of 20-in. (50-cm) and greater snowfall accumulations	High
				Category 3	Major – the typical major Northeast snowstorm, with large areas of 10-in. snows (generally between 50 and 150 × 103 mi2 with significant areas of 20-in. (50-cm) accumulations)	Medium
				Category 2	Significant - significant areas of greater than 10-in. (25-cm) snows while some include small areas of 20-in. (50-cm) snowfalls	Low
				Category 1	Notable – large areas of 4-in. (10-cm) accumulations and small areas of 10-in. (25-cm) snowfall	Negligible
		Heat	Heat Index (NOAA)	Extreme danger	Heat stroke or sunstroke are likely with continued exposure (over 130 °F)	High
				Danger	Sunstroke, heat cramps, and heat exhaustion are likely; heat stroke is possible (105–130 °F)	Medium
				Extreme caution	Sunstroke, heat cramps, and heat exhaustion are possible (90–105 °F)	Low
				Caution	Fatigue is possible with prolonged exposure and activity (80–90 °F)	Negligible

IT Sector Risk Assessment Methodology – Natural						
Threat Framework						
	Threat Category	Threat Criteria	Severity Scale	Criteria	Definition	Rating
		Hurricane	Saffir-Simpson Hurricane Scale (NOAA-National Hurricane Center)	Category 4/5	Extensive curtain wall failures, with some complete roof structural failure on small residences. Major erosion of beach areas and terrain may be flooded well inland as well	High
				Category 3	Structural damage to small residences and utility buildings, particularly those of wood frame or manufactured materials with minor curtain wall failures. Flooding near the coast destroys smaller structures, while larger structures are hit by floating debris	Medium
				Category 2	Damage to some roofing material, and also produce damage to poorly constructed doors and windows. Considerable damage is caused to vegetation, poorly constructed signs, and piers	Low
				Category 1	No significant damage to building structures. Minor coastal flooding and pier damage	Negligible
		Thunderstorm	Thunderstorm classification (NOAA-National Weather Service)	Supercell	Highly organized thunderstorm, posing a high threat to life and property	High
				Multicell line	Long line of storms with a continuous well-developed gust front at the leading edge of the line	Medium
				Multicell cluster	Group of cells, moving along as one unit, with each cell in a different phase of the thunderstorm life cycle	Low
				Single cell	Usually last between 20-30 minutes; not severe	Negligible
		Tornado	Fujita Tornado Damage Scale (NOAA-Storm Prediction Center)	Severe to incredible damage	Roofs and some walls torn off well-constructed houses; trains overturned; most trees in forest uprooted; heavy cars lifted off the ground and thrown (winds > 157 mph)	High

IT Sector Risk Assessment Methodology – Natural Threat Framework						
	Threat Category	Threat Criteria	Severity Scale	Criteria	Definition	Rating
				Considerable damage	Roofs torn off frame houses; mobile homes demolished; boxcars overturned; large trees snapped or uprooted; light-object missiles generated; cars lifted off ground (winds 113-157 mph)	Medium
				Moderate damage	Peels surface off roofs; mobile homes pushed off foundations or overturned; moving autos blown off roads (winds 73-112 mph)	Low
				Light damage	Some damage to chimneys; branches broken off trees; shallow-rooted trees pushed over; sign boards damaged (winds < 73 mph)	Negligible
		Wildfire	Haines Index (NOAA-National Weather Service)	High potential	Dry unstable lower atmosphere	High
				Moderate potential		Medium
				Low potential	Moist stable lower atmosphere	Low
				Very low potential		Negligible
		Fire	Normalized Burn Ratio (National Park Service)	High Severity	Normalized burn ratio between 660 and 1300	High
				Moderate-high Severity	Normalized burn ratio between 435 and 659	Medium
				Moderate-low Severity	Normalized burn ratio between 275 and 434	Low
				Low Severity	Normalized burn ratio between 100 and 274	Negligible
	Celestial	Geomagnetic Storms	Space Weather Scale (NOAA-Space Weather Prediction Center)	Severe to Extreme	Possible widespread voltage control problems and some protective systems will mistakenly trip out key assets from the grid	High
				Strong	Voltage corrections may be required, false alarms triggered on some protection devices	Medium
				Moderate	High-latitude power systems may experience voltage alarms, long-duration storms may cause transformer damage	Low
				Minor	Weak power grid fluctuations can occur	Negligible
		Solar Radiation Storms	Space Weather Scale (NOAA-Space Weather Prediction Center)	Severe to Extreme	Blackout of High Frequency (HF) radio communications through the polar regions and increased navigation errors over several days are likely	High

IT Sector Risk Assessment Methodology – Natural						
Threat Framework						
	Threat Category	Threat Criteria	Severity Scale	Criteria	Definition	Rating
				Strong	Degraded HF radio propagation through the polar regions and navigation position errors likely	Medium
				Moderate	Small effects on HF propagation through the polar regions and navigation at polar cap locations possibly affected	Low
				Minor	Minor impacts on HF radio in the polar regions	Negligible
		Radio Blackouts	Space Weather Scale (NOAA-Space Weather Prediction Center)	Severe to Extreme	HF radio communication blackout on most of the sunlit side of Earth for one to two hours. HF radio contact lost during this time	High
				Strong	Wide area blackout of HF radio communication, loss of radio contact for about an hour on sunlit side of Earth	Medium
				Moderate	Limited blackout of HF radio communication on sunlit side, loss of radio contact for tens of minutes	Low
				Minor	Weak or minor degradation of HF radio communication on sunlit side, occasional loss of radio contact	Negligible

IT Sector Risk Assessment Methodology – Natural				
Vulnerability Framework				
	Vulnerability Factors	Definition	Criteria	Rating
Assess Applicability of Vulnerabilities	People Process Technology Physical Other	How well do vulnerability(-ies) align with threat requirements (based on a threat's intent, capabilities, and/or operational constraints)?	Vulnerability(-ies) are well aligned with the threat requirements and can easily be exploited	High
			Vulnerability(-ies) are not optimal for the threat, but can be adapted for use with some effort	Medium
			Vulnerability(-ies) are not well suited to the threat requirements, but can be used if they are the only opening	Low
			Vulnerability(-ies) are essentially useless to the threat	Negligible
Assess Simplicity of Vulnerabilities	People Process Technology Physical Other	How easily can vulnerability(-ies) be exploited?	Very simple, vulnerability(-ies) can be exploited with limited resources	High
			Some general training or modest resources would be needed to exploit vulnerability(-ies)	Medium
			Specialized training or resources are needed to exploit the vulnerability(-ies)	Low
			Exploiting vulnerability(-ies) is complex and requires extensive training and significant resources	Negligible

IT Sector Risk Assessment Methodology – Natural				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
Assess Impact to Critical IT Sector Function	Confidentiality, Integrity, and Availability	Confidentiality	The unauthorized disclosure of information residing on information systems that support the critical function	
		Integrity	The unauthorized modification or destruction of the function	
		Availability	The disruption of access to or use of the function	
Assess Impact to Function's Information Systems	STRIDE	Spoofing	The assumption of other user accounts, or the attributes of another user	
		Tampering	The unauthorized alteration of data and system resources in inappropriate ways or by the inappropriate people	
		Repudiation	The dishonest denial of actions performed	
		Information Disclosure	The unauthorized access of data	
		Denial of Service	The inaccessibility of systems that perform acceptably when needed	
		Elevation of Privilege	The unauthorized increase of user privileges	
Determine if the Consequence will Cascade Beyond the Function	Time required to detect the incident	Predictive	The threat will be identified before the incident occurring	
		Real-time	N/A	
		Minutes	N/A	
		Hours	N/A	
		Days	N/A	
		Months	N/A	
	Time required to recover the function	Real-time	Accounts for mitigations that anticipate and preclude consequences	
		Minutes	Accounts for mitigations due to redundancy that enable continued real time services	
		Hours	Accounts for mitigations due to backup and redundancy	
		Days	Accounts for mitigations due to Continuity of Operations (COOP) Planning	
		Months	Accounts for mitigations due to other contingency planning efforts	
	Time required to reconstitute the function	N/A	Reconstitution of the function will not occur	
		Real-time	Accounts for mitigations that anticipate and preclude consequences	
		Minutes	Accounts for mitigations due to redundancy that enable continued real time services	
		Hours	Accounts for mitigations due to backup and redundancy	

IT Sector Risk Assessment Methodology – Natural				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
		Days	Accounts for mitigations due to Continuity of Operations (COOP) Planning	
		Months	Accounts for mitigations due to other contingency planning efforts	
	Time to recover from the incident	Real-time	N/A	
		Minutes	N/A	
		Hours	N/A	
		Days	N/A	
		Months	N/A	
Assess Cascading Consequences Beyond Function - Government Essential Functions	Executive (Federal)	Foreign policy	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		National security/Defense	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Homeland security	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Revenue collection and spending	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Legislative (Federal)	Regulating taxing	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Regulating spending	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Grant necessary powers/funding for executive orders	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Judicial (Federal)	Court system	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	State/Local	Education	Mission is severely degraded	High
			Some mission degradation will occur	Medium

IT Sector Risk Assessment Methodology – Natural				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Medicaid	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Economic Security	18 CIKR sectors	Agriculture and Food	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Banking and Finance	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Chemical	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Commercial Facilities	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Commercial Nuclear Reactors, Materials and Waste	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Communications	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Critical Manufacturing	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Dams	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Defense Industrial Base	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Drinking Water and Water	Mission is severely degraded	High

IT Sector Risk Assessment Methodology – Natural				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
		Treatment Systems	Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Emergency Services	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Energy	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Government Facilities	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Information Technology	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		National Monuments and Icons	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Postal and Shipping	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Public Health and Healthcare	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Transportation Systems	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Public Health and Safety Missions	Emergency service missions	Emergency management (E911)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Fire, search, and rescue	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low

IT Sector Risk Assessment Methodology – Natural				
Consequence Framework				
	Consequence Factor	Criteria	Definition	Rating
			No identifiable effect on mission	Negligible
		Law enforcement	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Emergency medical services	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
	Non-emergency service missions	Welfare needs (e.g., shelter, food, and water)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Medical incident management/containment	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Energy	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Communications	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
Assess Cascading Consequences Beyond Function - Public Confidence Missions	Public confidence	Communication between the government and the public	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Confidence in corporate entities (measured by public awareness of corporate entities involved)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Confidence in government and economy (measured by public awareness of impact)	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible
		Corporate and government confidence and ability to continue investing in new and evolving technologies	Mission is severely degraded	High
			Some mission degradation will occur	Medium
			Only slight effect on mission	Low
			No identifiable effect on mission	Negligible