Information Technology Sector

Risk Management Strategy for the

Provide Domain Name Resolution Services Critical Function

June 2011

Contents

Executive Summary i
1 Information Technology Sector Risk Management Overview 1
2 Risk Overview – *Provide Domain Name Resolution Services* Critical Function 2
3 Provide Domain Name Resolution Services Risk Management Strategy 4
3.1 Risk of Concern – Information Disclosure/Privacy Loss (Manmade Unintentional) 6
3.1.1 Risk Overview 6
3.1.2 Risk Response 7
3.2 Risk of Concern – Policy Failure: Breakdown of Single, Interoperable, Global Internet (Manmade Deliberate) 10
3.2.1 Risk Overview 10
3.2.2 Risk Response 11
3.3 Risk Response to Large Scale Attack on Infrastructure: Denial of Service (Manmade Deliberate) 16
3.3.1 Risk Overview 16
3.3.2 Risk Response 18

Figures

Figure 1: Provide Domain Name Resolution Services Attack Tree (Summary) 3
Figure 2: Provide Domain Name Resolution Services Relative Risk Table 4
Figure 3: Information Disclosure/Privacy Loss (DNS 3) 7
Figure 4: Effectiveness of Proposed Mitigation Strategy to Information Disclosure/Privacy Loss 8
Figure 5: Breakdown of Single, Interoperable, Global Internet (DNS 1) 11
Figure 6: Effectiveness of Proposed Mitigation Strategy to Breakdown of Single, Interoperable, Global Internet 15
Figure 7: Denial of Service by Large Scale Attack on Infrastructure (DNS 2a) 18
Figure 8: Effectiveness of Proposed Mitigation Strategy to Large Scale Attack on Infrastructure 20

Tables

Table 1: DNS Risk and Mitigation Overview ii
Table 2: IT Sector's High Consequence Risks for DNS 2
Table 3: DNS Risk and Mitigation Overview 5
Table 4: Feasibility of Proposed Mitigation Strategy to Information Disclosure/Privacy Loss 9
Table 5: Feasibility of Proposed Mitigation Strategy to the Breakdown of Single, Interoperable, Global Internet 16
Table 6: Feasibility of Proposed Mitigation Strategy to Large Scale Attack on Infrastructure 21

Executive Summary

Public and private Information Technology (IT) Sector owners and operators completed the first-ever functions-based risk assessment in August 2009. The IT Sector Baseline Risk Assessment (ITSRA) assesses risks from manmade deliberate, manmade unintentional, and natural threats using threat, vulnerability, and consequence frameworks within the Sector's risk assessment methodology. The ITSRA resulted in a comprehensive baseline IT Sector Risk Profile that identifies national-level risks of concern for the IT Sector. Public and private sector partners collaboratively developed the assessment, which reflects participating subject-matter experts' (SME) expertise and collective consensus.

Critical IT Sector Functions

Provide IT products and services

Provide incident management capabilities

Provide domain name resolution services

Provide identity management and associated trust support services

Provide Internet-based content, information, and communications services

Provide Internet routing, access, and connection services

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

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

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

The remainder of this document:

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

Table 1: DNS Risk and Mitigation Overview

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings[1]
Information Disclosure/ Privacy Loss	Low likelihood; low consequence	❑ Restricting zone transfers to known and trusted partners ❑ Implementing DNS data and configuration practices ❑ Conducting education and training ❑ Adopting standards and best practices	Negligible likelihood; negligible consequence
Policy Failure: Breakdown of Single, Interoperable Global Internet	Medium likelihood; high consequence	❑ Implementing Internationalized Domain Names (IDN) ❑ Using global forums to discuss DNS security issues ❑ Promoting a DNS dashboard ❑ Leveraging the results of cross constituency, internationally-supported studies ❑ Increasing information sharing to build confidence across the DNS community ❑ Developing and implementing automation software to process root zone changes ❑ Establishing 'norms of behavior' for cyberspace ❑ Increasing confidence in the overall system through developing and implementing Resource Public Key Infrastructure (RPKI) ❑ Establishing a Domain Name System-Computer Emergency Response Team (DNS-CERT) capability ❑ Creating a unilateral resolution ❑ Increasing confidence in the DNS infrastructure through implementing Domain Name System Security Extensions (DNSSEC) at the root and top-level domain (TLD) levels ❑ Enhancing national-level modeling and simulation ❑ Conducting exercises to test DNS services (e.g., a day without the Internet)	Low likelihood; high consequence

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

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings[1]
Large Scale Attack on Infrastructure: Denial of Service	Low likelihood; high consequence	❑ Performing a gap analysis ❑ Adopting standards and best practices ❑ Developing a DNS dashboard ❑ Pursuing diplomatic and law enforcement responses ❑ Improving emergency communications ❑ Enhancing national-level modeling and simulation ❑ Conducting exercises to test DNS services (e.g., a day without the Internet)	Low likelihood; high consequence

The finalized RMA strategies will inform the 2011 IT Sector Annual Report (SAR), which is the primary document that outlines Critical Infrastructure and Key Resources (CIKR)-sector research and development (R&D) efforts and priorities. The SAR will include sector cybersecurity R&D requirements, which will serve as inputs into the Department of Homeland Security (DHS) Science and Technology Directorate's (S&T) processes for identifying and addressing R&D needs. The report will also influence cross-sector cybersecurity R&D needs, requirements, and recommendations to those areas where the U.S. Government should make focused investments.

Additionally, the recommendations will be introduced to the Cyber Security and Information Assurance Interagency Working Group (CSIA IWG), which provides a forum for Federal Departments/Agencies to exchange program-level R&D information. The IT Sector maintains an active relationship with the CSIA IWG and will use the results and recommendations in this report to coordinate those key points of concern where both groups can work together to develop targeted R&D efforts.

Further, several key public forums will be discussing issues that will shape and influence—both now and in the future—the DNS space, and will likely affect recommendations in this strategy. A list of identified organizations and meetings appears at the end of this document.

The IT Sector's Metrics Working Group is currently working with the Protective Programs and Research and Development Working Group (PPRD WG) to identify SMEs and develop strategies for the remaining functions as outlined in the ITSRA. This report, coupled with similar efforts across the other critical functions, will provide a foundation for comprehensive IT Sector national-level risk reduction.

1 Information Technology Sector Risk Management Overview

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

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

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

The IT Sector Baseline Risk Assessment (ITSRA), released in 2009, serves as the foundation for the Sector's national-level risk management activities.[2] Government and private sector partners collaborated to conduct the assessment, which reflects the expertise and collective consensus of participating subject matter experts (SMEs). The ITSRA methodology assesses risks from manmade deliberate, manmade unintentional, and natural threats that could affect the ability of the Sector's critical functions and sub-functions to support the economy and national security. The methodology leverages existing risk-related definitions, frameworks, and taxonomies from a variety of sources, including public and private IT Sector partners, standards development organizations, and policy guidance entities. By leveraging these frameworks, the Sector's methodology reflects current knowledge about risk and adapts them in a way that enables a functions-based risk assessment.

The following table highlights the IT Sector's high consequence risks within the *Provide Domain Name Resolution Services* (i.e., DNS) function. SMEs identified these risks 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 that could impact the confidentiality, integrity, or availability of the critical function. The *Mitigations* column is a summary of the mitigations identified in the ITSRA and were later validated through follow-on IT Sector Risk Management (ITSRM) sessions to address the highlighted risks.

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

Table 2: IT Sector's High Consequence Risks for DNS

Critical IT Sector Function	Risks of Concern	Mitigations (Existing, Being Enhanced, or Potential Future)
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*

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

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

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

2 Risk Overview – *Provide Domain Name Resolution Services* Critical Function

***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 may 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 convert and resolve 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 an IP address, which is more difficult to remember. 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 IP addresses require the ability to look up host names and addresses, the DNS is as critical to the Internet as data transmission lines.

The Government and private sector 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, top-level domains (TLD), and lower-level Domain Services;
- Provide DNS Provisioning;
- Provide Name Resolution Services for Client Hosts; and
- Provide Security and Incident Management for DNS Operations.

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

As detailed in Figure 1, 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.

Figure 1: Provide Domain Name Resolution Services Attack Tree (Summary)

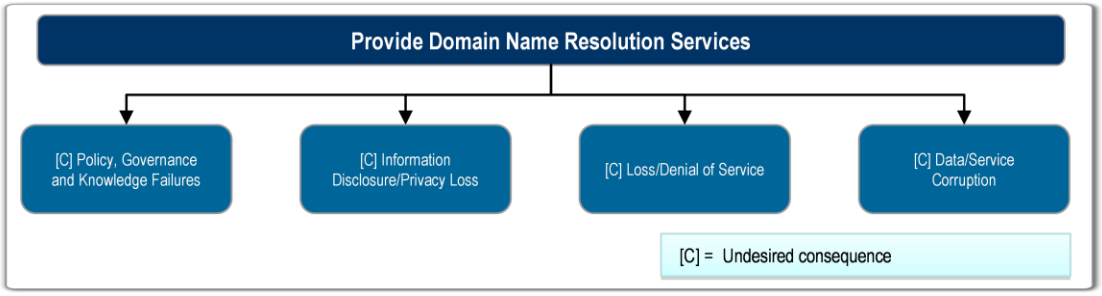
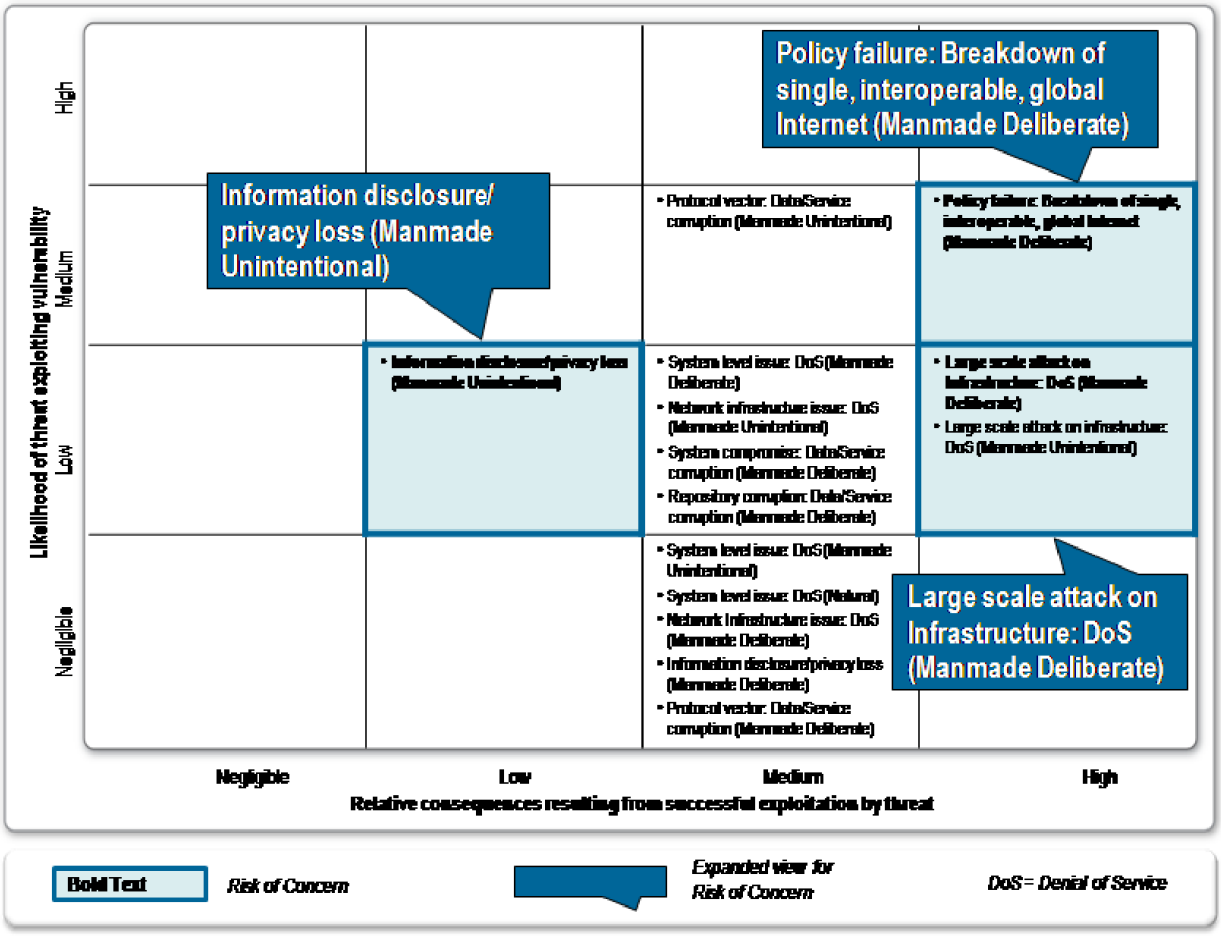


Figure 2 shows the risk profile for the *Provide Domain Name Resolution Services* critical function that 2009 ITSRA participants developed. This matrix maps the likelihood of each threat exploiting a DNS threat (Y-axis) against the relative consequences of that threat exploiting vulnerability (X-axis).

Figure 2: Provide Domain Name Resolution Services Relative Risk Table



3 Provide Domain Name Resolution Services Risk Management Strategy

The following three sections (Sections 3.1, 3.2, and 3.3) describe proposed risk mitigation strategies for the three most prominent DNS risks. The ITSRA identified those risks as:

- Information Disclosure/Privacy Loss (Manmade, Unintentional)[3]
- Policy Failure: Breakdown of Single, Interoperable Global Internet (Manmade, Deliberate)
- Large Scale Attack on Infrastructure: Denial of Service (Manmade, Deliberate)[4]

IT Sector partners resolved to pursue a mitigation approach for each of the DNS risks under consideration.

Table 3 illustrates the risk mitigation activities associated with each examined risk of concern.

[3] While the *Information Disclosure/Privacy Loss* risk did not emerge as a risk of concern based strictly on likelihood and consequence factors, IT Sector partners addressed the risk as part of this report based on the Sector's ability to implement RMAs to effectively reduce the risk of manmade unintentional data disclosure.
[4] The group did not have time to directly discuss manmade, unintentional risks to the infrastructure and focused the majority of their time discussing manmade, deliberate risks.

Table 3: DNS Risk and Mitigation Overview

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings[5]
Information Disclosure/ Privacy Loss	Low likelihood; low consequence	❑ Restricting zone transfers to known and trusted partners ❑ Implementing DNS data and configuration practices ❑ Conducting education and training ❑ Adopting standards and best practices	Negligible likelihood; negligible consequence
Policy Failure: Breakdown of Single, Interoperable Global Internet	Medium likelihood; high consequence	❑ Implementing Internationalized Domain Names (IDN) ❑ Using global forums to discuss DNS security issues ❑ Promoting a DNS dashboard ❑ Leveraging the results of cross constituency, internationally-supported studies ❑ Increasing information sharing to build confidence across the DNS community ❑ Developing and implementing automation software to process root zone changes ❑ Establishing 'norms of behavior' for cyberspace ❑ Increasing confidence through developing and implementing Resource Public Key Infrastructure (RPKI) ❑ Establishing a Domain Name System-Computer Emergency Response Team (DNS-CERT) capability ❑ Creating a unilateral resolution ❑ Implementing Domain Name System Security Extensions (DNSSEC) at the root ❑ Enhancing national-level modeling and simulation ❑ Conducting exercises to test DNS services (e.g., a day without the Internet)	Low likelihood; high consequence

[5] Assumes complete implementation of the items noted in the *Risk Mitigation Activities* column.

Risk	ITSRA Likelihood and Consequence Ratings	Risk Mitigation Activities	Resulting Likelihood and Consequence Ratings[5]
Large Scale Attack on Infrastructure: Denial of Service	Low likelihood; high consequence	❑ Performing a gap analysis ❑ Adopting standards and best practices ❑ Developing a DNS dashboard ❑ Pursuing diplomatic and law enforcement responses ❑ Improving emergency communications ❑ Enhancing national-level modeling and simulation ❑ Conducting exercises to test DNS services (e.g., a day without the Internet)	Low likelihood; high consequence

3.1 Risk of Concern – Information Disclosure/Privacy Loss (Manmade Unintentional)

3.1.1 Risk Overview

Protecting the confidentiality of information can temper an attack's overall consequences. Risk assessment SMEs identified two methods by which information could be disclosed:

- Recursive infrastructure: Recursive infrastructure refers to how most DNS query responses are rendered. The majority of DNS query responses are generated from the cache of recursive servers, which obtains the IP address of the site or computer a user attempts to reach via a DNS query. Threat actors can potentially exploit weaknesses in recursive server code and redirect traffic.
- Cache disclosure: DNS servers cache hostname to IP address mapping in their memory. If threat actors accessed or obtained a DNS servers' cached hostname to IP address mapping data, the actor could manipulate the data to impact how DNS queries were resolved, erroneously and potentially fraudulently redirecting Internet traffic.

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 Universal Serial Bus memory keys;
- Poor or negligent software development practices;
- Phishing attacks; and
- Non-secure wireless networks (e.g., hotel or other guest type networks).

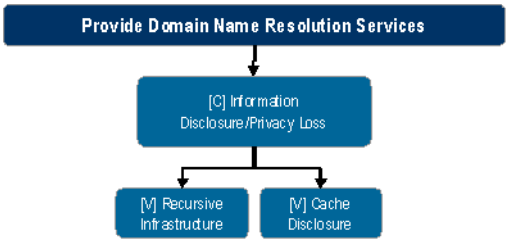
During DNS SME risk management discussions, IT Sector partners chose to narrow the aperture of potential information disclosure concerns to the first two bullet points highlighted above. Since the operators of root DNS servers monitor the infrastructure continuously, they have easy access to logs and/or caches and the ability to send all or part of these logs and/or caches to other personnel and trusted members of the DNS community. This movement creates additional opportunities for unintentional information disclosure. When personnel do not follow correct data protection procedures or are negligent, malicious actors can exploit vulnerabilities and potentially access log and/or cache information.

Furthermore, not all zone files and/or caches are properly configured and may contain unnecessary or sensitive information that could lead to individual or corporate privacy loss. An unintended "zone transfer" could give an attacker a copy of DNS records, indicating the addresses, aliases, and identities of objects in the DNS. An attacker can exploit this information with the intent to compromise or steal Internet data.

Organizations must implement broader quality control practices, comprehensive code reviews, and consistent deployment procedures to prevent negative impacts to the integrity of information and information privacy. Personnel must be trained sufficiently to recognize malicious attempts to solicit information and/or identify social engineering methods in which actors compromise security. Without this training, personnel may not be able to thwart an attack.

ITSRA SMEs developed the following attack tree to scope the IT Sector's risk response strategy to information disclosure/privacy loss.

Figure 3: Information Disclosure/Privacy Loss (DNS 3)



3.1.2 Risk Response

The ITSRA established that the national-level risk of a manmade, unintentional information disclosure/privacy loss is *low likelihood* and *low consequence* (see Figure 2). IT Sector partners agreed that the appropriate risk response for this particular risk of concern requires a combined mitigation strategy, including:

- Restricting zone transfers to known and trusted partners: Public-zone transfers are legal by default and provide information to all interested parties equally. Sharing the root zone file with others is very low risk because the root zone is small and does not change frequently; accepting this risk is inherent to DNS operation. However, the case may be different for zones where significant monetary value is attached (for example, .com), where access to the zone file might be restricted or contain a significant amount of sensitive information. The zone's construction should determine the level of trust; if sensitive information is protected, then sharing the information more freely is less likely to have adverse consequences. Modern configurations restrict zone transfers, but the legacy of open information sharing has been difficult to overcome.[6]

- Implementing DNS data and configuration practices: Sensitive information leakages can occur when zones are mis-configured. To combat this, users should populate the DNS with correct information and omit sensitive information, such as classifying information that links to specific staff or management personnel. Poorly-configured zones can lead to the disclosure of sensitive information, which malicious actors could use to prepare for a cyber or physical attack. The information outsiders gain would be minimal if population and configuration is properly executed.

[6] The Internet Corporation for Assigned Names and Numbers (ICANN) recently published a Strategy Paper on Zone File Access for the Future: http://www.icann.org/en/topics/new-gtlds/zfa-strategy-paper-12may10-en.pdf.

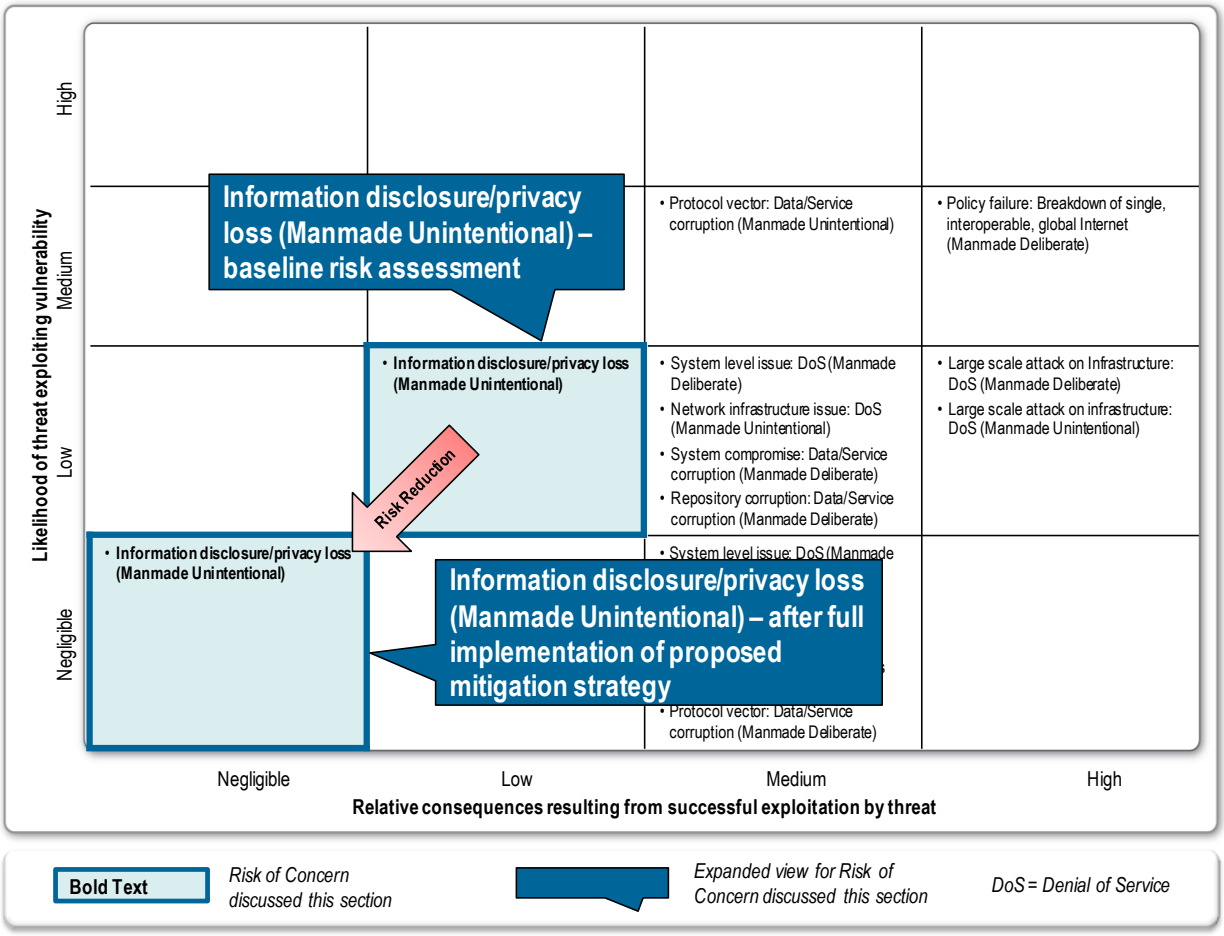
DNS data relevant only to the internal workings of a group or company (such as a printer name) should be confined to zones only accessible from internal networks.

- Conducting education and training: DNS-related training and education programs currently exist but could be enhanced to focus on negative publicity resulting from data file misuse (both intentional and unintentional). Adequate network administrator training will diminish or elimate the consequence because stakeholders would be less likely to introduce unnecessary or sensitive information into the system.

- Adopting standards and best practices: The United States Government (USG) should focus its DNS risk management efforts internally before advising foreign nations on best practices. Efforts may include creating a set of standards or promoting best practices for secure and trusted zone transfer processes.

Organizations can accomplish these activities with existing resources; no additional R&D is required. After formulating the combined risk mitigation strategy, IT Sector partners concluded that full nation-wide implementation of the proposed mitigation steps above would reduce the national-level risk to *negligible likelihood* and *negligible consequence* (see Figure 4).

Figure 4: Effectiveness of Proposed Mitigation Strategy to Information Disclosure/Privacy Loss



IT Sector partners were able to reach consensus on the feasibility of implementing the proposed risk management strategy (see Table 4). IT Sector partners noted the following key feasibility considerations:

- Legislative action may be needed to foster risk response implementation;
- The Sector would not be able to enforce implementation on those organizations that do not fall under existing regulations (e.g., the Federal Information Security Management Act [FISMA] or Sarbanes-Oxley Act [SOX]).
- Auditing could work on a small scale but would be difficult on a national or international scale;
- The Sector could use automated queries to determine if organizations have implemented standards; and
- A third party can never determine the importance of the information being transferred.

IT Sector partners noted that a slight degradation may occur to *Provide Internet Routing, Access, and Connection Services* and the *Provide Internet-based Content, Information, and Communications Services* critical functions due to more secure zone transfers. Also, the number of stakeholders responsible for managing keys will increase, thus slowing down the availability of these critical functions. The IT Sector may consider adding an auditing function to ensure standards are implemented, ultimately measuring the RMAs' effectiveness. Furthermore, IT Sector partners should analyze the risk mitigation strategy in greater detail to determine feasibility, implementation progress, and effectiveness measures related to this particular risk of concern.

Table 4: Feasibility of Proposed Mitigation Strategy to Information Disclosure/Privacy Loss

Feasibility Rating	Feasibility Factors	Description	Criteria
High	**Legal**	Statutes, regulation	The existing legal framework is favorable for implementing the proposed risk response.
High	**Organizational Compliance**	Best practices, organizational charters, corporate values	The implementation of the proposed risk response aligns closely with existing standards and best practices.
High	**Political**	Public confidence, privacy-related issues	The risk response is politically viable.
Medium	**Financial**	Cost, budget limitations	Total average life-cycle costs for implementing the risk response can only be partially covered via market forces and existing business models.
Low	**Time**	Reasonable schedule expectations	The implementation of the proposed risk response will take a relatively longer time frame (i.e., 24 months or longer for full implementation).
High	**Technology**	Ease of implementing existing technology or developing new technology	In the context of technological viability, the risk response is relatively easy to implement or develop.
High	**Market**	Market conditions, competition	The market conditions are favorable for implementing the risk response.
Medium	**Compatibility**	Confidentiality, Integrity, and Availability after implementation	Some compatibility issues are associated with implementing the risk response.
Low	**Cultural**	The alignment of IT Sector culture and the risk response	The IT Sector's cultural environment does not facilitate the risk response.

3.2 Risk of Concern – Policy Failure: Breakdown of Single, Interoperable, Global Internet (Manmade Deliberate)

3.2.1 Risk Overview

The Internet is an open, interoperable, global system that has yielded unprecedented economic growth and innovation. Breakdown of the single root zone structure and the creation of alternate roots would have significant implications to international trade since the global free flow of electronic information would be hampered.

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

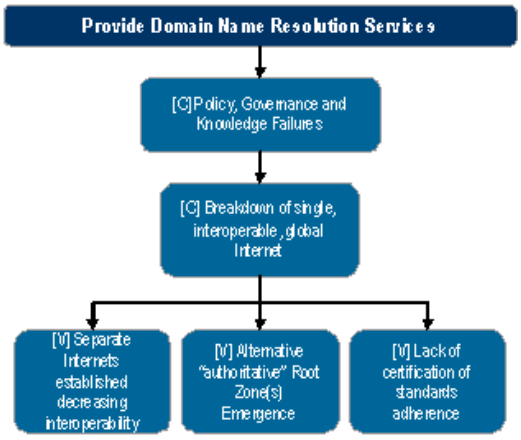
- Politically-motivated attempts to influence or disrupt DNS operations;
- Desire for financial gain;
- Demonstration of technical superiority; and
- Gratuitous defacement or damage.

In previous ITSRA DNS discussions, IT Sector SMEs focused on root fragmentation risk threat scenarios. However, in the sessions leading up to this report, IT Sector partners scoped the risk management discussion to focus on the conditions and implications of an alternate root structure through opportunistic means. Establishing regional or alternative Internets could decrease interoperability and cause technical confusion. Such a situation could cause strategic consequences across multiple sectors. Due to strong global network effects, all prior attempts to fragment the root have failed. Any actor who 'secedes' from the compatible root must overcome enormous inertia and coordinate several actors to gain recognition. Even if the actor succeeds in these activities, the benefits of remaining interoperable with the existing root far outweigh the task of operating in a fragmented, disconnected root. However, if the political, strategic, or economic environment provides an opportunity to establish and manage an alternative root system, this situation could change.

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 significantly improve. In addition, nation-states may want to capitalize on the perceived control of the United States over the Internet by offering a competing authoritative root (resulting in Internet fragmentation) to undermine the perceived hegemony of the United States. If Internet users become dependent on the alternate root, actors would then gain political and economic advantage, which could have larger implications to the global economy.

ITSRA SMEs developed the following attack tree to scope the IT Sector's risk response strategy to the breakdown of a single, interoperable, global Internet.

Figure 5: Breakdown of Single, Interoperable, Global Internet (DNS 1)



3.2.2 Risk Response

The ITSRA established that the national-level risk of a manmade deliberate breakdown of a single, interoperable, global Internet as being *medium likelihood* and *high consequence* (see Figure 2). IT Sector partners agreed that organizations should implement collectively the policy and technology responses below, since no one response solves all of the concerns:

- Implementing Internationalized Domain Names (IDN): A broad range of countries, territories, and communities—many of which have criticized the current management of the Internet's unique identifier system—hailed the introduction of IDNs in the root. IDN implementation could help reduce the likelihood of root fragmentation because it promotes inclusion across the Internet by allowing for Internet users and communities, whose primary language is not based on Latin characters—known as American Standard Code for Information Interchange (ASCII)—to reflect their own language and script identity through the introduction of non-ASCII characters into the root. Introducing IDNs would allow other cultures/countries with non-Latin based languages and character sets to have a sense of ownership or control over their pieces of the Internet and allow disparate corners of the globe to connect to the Internet in their local languages. This solution addresses concerns from certain communities that have been most vocal and may have sought to utilize alternate root systems if their concerns had not been met. The Internet Corporation for Assigned Names and Numbers' (ICANN) first implementation phase involves a fast track process to introduce a limited number of IDNs country-code TLDs into the root. Currently, ICANN has approved 13 country and territory applications in the evaluation phase, and several IDN strings have entered into the root zone, all of which could relieve foreign pressure to develop an alternate root system.[7]

- Using global forums to discuss DNS security issues: Activities such as the DNS Symposium on Security, Stability, and Resiliency (DNS SSR) bring stakeholders together from around the world to discuss key issues impacting the Internet from a variety of technical and policy-related perspectives. The second DNS SSR Symposium, which took place in February 2010 in Kyoto, Japan, built upon the first symposium's foundational work and sought to answer questions related to understanding the DNS' "health" and ways to measure its current state, identifying gaps in

[7] For more information on the IDN Fast Track Process, including which strings have passed and are being entered into the Root, please see: http://www.icann.org/en/topics/idn/fast-track/string-evaluation-completion-en.htm.

existing techniques, and recommending improvements to DNS systems condition monitoring.[8] Symposium attendees included participants from: the Asia-Pacific Network Information Center, Canada, China, European Network and Information Security Agency, ICANN, Japan, the Netherlands, New Zealand, Réseaux IP Européens, Singapore, Sweden, the United Kingdom, the United States, and others. Participants released a final report on symposium findings that highlighted key security concerns.[9]

- Promoting a "DNS Dashboard": 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 operation centers to anticipate and protect DNS infrastructure from malware attacks. An integrated DNS dashboard (or confidence index) has the potential to provide real-time global monitoring of the DNS' entire "health" and could be used to measure DNS health. Developing a DNS dashboard would allow for increased transparency around DNS management and indicate whether the system is functioning as anticipated.

- Leveraging the results of cross constituency, internationally-supported studies: Organizations should actively support widely-respected reports and studies undertaken by the Internet community, implementing report recommendations to improve the Internet infrastructure. For example, organizations could incorporate the results of the ICANN-sponsored Root Scaling Study into ongoing and future technical and policy-making decisions regarding the scalability of the root zone, given various changes.[10]

- Increasing information sharing to build confidence across the DNS community: Currently, DNS information is shared on a predominantly ad hoc basis. More formalized information sharing channels would add stability and transparency to the somewhat opaque process of DNS management. For example, allowing for information to be shared among ICANN, the root zone operators, and the Root Service System Advisory Committee (a sub-structure of ICANN), and other relevant parties regarding changes to the root—such as the implications for introducing DNSSEC, new global Top Level Domains (gTLDs), IDNs, and IP version 6 (IPv6) at the root-level—could increase confidence across the DNS community and build trust in the present structure's stability.

- Developing and implementing automation software to process root zone changes: Most governments want an interoperable, global root structure, but they also want to be in a peer position with the USG for oversight authority because of the perceived dominant United States position over the authoritative root structure. Automating the root zone change, authorization, and implementation process can be a means of "depoliticizing" changes to the root zone by lessening the perceived footprint of all three members of the update process (VeriSign, the USG, and ICANN). Implementing an automated Internet Assigned Numbers Authority (IANA) function is currently in progress to address this issue.

- Establishing "norms of behavior" for cyberspace: Since many nations are engaged in a Cyber competition that may adversely affect the DNS, nations must develop and adhere to common measures that will ensure that the DNS will continue to operate successfully under stressful

[8] For more information on the first Global DNS SSR Symposium, including the final report, please see: http://www.gtisc.gatech.edu/icann09.

[9] "The Global DNS Security, Stability, & Resiliency Symposium: Summary, Trends, and Next Steps". Final Report. April 2, 2010. http://www.gtisc.gatech.edu/pdf/DNS_SSR_Symposium_Summary_Report.pdf.

[10] Root Scaling Study Team. "Scaling the Root: Report on the Impact on the DNS Root System of Increasing the Size and Volatility of the Root Zone". Final report prepared for the Root Scaling Steering Group. September 7, 2009. https://st.icann.org/data/workspaces/new-gtld-overarching-issues/attachments/security_and_stability_root_zone_scaling:20091007231001-0-13653/original/root-scaling-study-report-31aug09-en.pdf.

conditions. Examples of "norms" that would benefit the DNS are: creating an international Joint Cyber Risk Reduction Center that would (1) serve as a focal point for sharing information, (2) act as an intermediary during times of crisis, and (3) include support by people from competing nations to help reduce emerging tensions; criminalizing the distribution of offensive cyber attack weapons by private citizens of each nation; and maintaining a mutually agreed-upon cyber early warning system.

- Increasing confidence in the overall system through developing and implementing RPKI: To date, the Internet has operated without a secure means to certify the allocation of Internet number resources, particularly Autonomous System Numbers (ASN) and IP addresses. The pending exhaustion of the IPv4 address space, coupled with a pressing need to improve the security of the global Internet routing system, has given impetus to the development of a resource certification infrastructure for the Internet. A consistent shared view around the world of which number resources are allocated to whom is essential for the reliable operation of the Internet as it continues to grow. The Internet Engineering Task Force (IETF) Secure Inter-domain Routing (SIDR) Working Group (WG) has been working with the various stakeholders to specify a RPKI system that can be used to certify these resource allocations in order to substantially improve the security of the routing system, and thus add confidence to the DNS system. The Internet Architecture Board (IAB) has recommended that the IANA functions contractor become the trust anchor for the RPKI system.[11] However, ARIN and the Number Resources Organization (NRO), a representative body of the Regional Internet Registries, have indicated their support for a single trust anchor for the RPKI system, but they have not identified a specific organization.[12]

- Establishinga DNS-CERT capability:[13] To increase incident management coordination and collaboration, and to protect the entire DNS infrastructure, the Internet community has proposed developing a DNS-CERT capability; the community is currently determining the exact need for, and scope, roles, and responsibilities of such a capability. Suggestions range from serving a strictly DNS incident response function that involves all members of the DNS operator community to increasing information sharing/education regarding the importance of the DNS and managing vital threat information related to the DNS. As the Internet matures, operators require more effective mechanisms to enable them to work together to manage an incident affecting the DNS, as well as ensure overall trust in the system is maintained.[14]

- Creating a unilateral resolution: A potential resolution is for the DNS community to adopt an unwavering, stated policy that it will not tolerate alternative roots and will instead rely on the status quo structure with collaborative improvements.

In addition to the IT Sector partners' potential enhanced and future mitigation recommendations found in the ITSRA, the Internet community could employ the following mitigation activities:

- Increasing confidence in the DNS infrastructure through Implementing DNSSEC at the Root and TLD Levels: DNSSEC mitigates the risk of "man-in-the-middle" attacks, providing a "chain of trust" from the root zone to the end path name server so an end user can verify the validity of the resolution path 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 can cryptographically validate the signatures. If

[11] See: http://www.ietf.org/mail-archive/web/ietf-announce/current/msg07028.html.
[12] See: https://www.arin.net/about_us/bot/bot2009_0206.html and http://www.nro.net/news/nro-declaration-rpki.html.
[13] See: http://icann.org/en/topics/ssr/dns-cert-business-case-19mar10-en.pdf.
[14] Instead of developing a DNS-CERT capability, another option would be to enhance the mission of an existing organization such as DNS-OARC, which is already involved in information sharing, etc. within the DNS operator community but whose mission might be more narrowly focused. For information on DNS-OARC, please see: https://www.dns-oarc.net/.

the signatures are determined to be invalid, the end user's application may disregard the result or warn the user that the signature did not validate.

For DNSSEC to be deployed successfully and its benefits fully realized, DNSSEC needs to be deployed at the root-level and down the Internet hierarchy to create a complete "chain of trust"; that is, from the start of a DNS query through all name servers and caching resolvers, and back to the end user. A deliberately-unvalidatable root zone was initially deployed at all 13 root zones as a means of testing the underlying infrastructure and determining capacity and load capabilities. It is expected that DNSSEC will be fully implemented at the root zone on July 15, 2010.[15] DNSSEC is not a panacea; it is a technical solution to a defined set of technical problems that tries to increase confidence in the DNS, and thus, the overall Internet infrastructure.

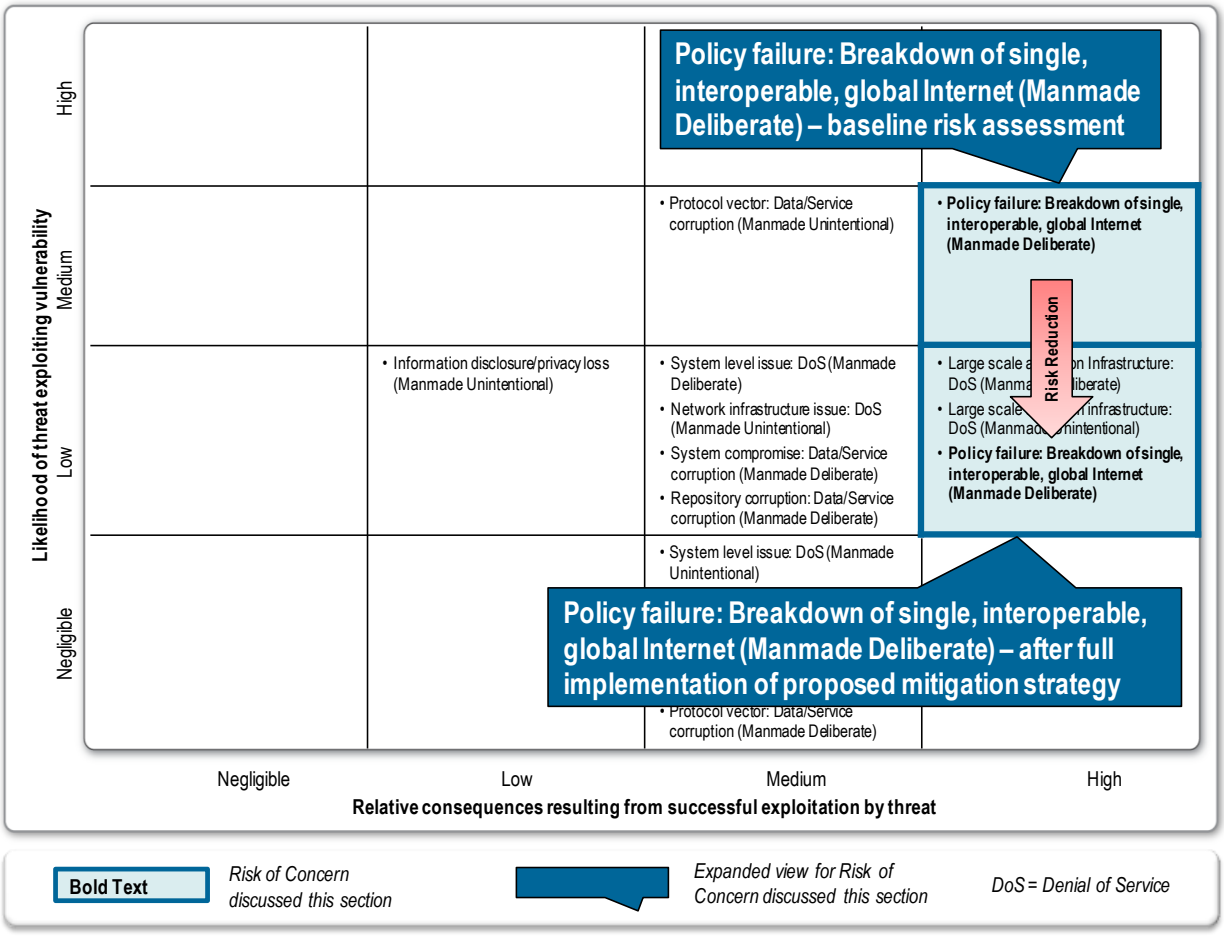
- Enhancing national-level modeling and simulation capabilities: To better understand and respond to pressures and impacts on the DNS, modeling and simulation of threats to the DNS is necessary. Such modeling and simulation should include IPv6, DNSSEC, IDN, and additional TLD impacts. National-level and multi-discipline modeling and simulation efforts could assist in developing a more unified effort to mitigate accidental risks. These efforts could encourage investment in new technologies to expand beyond the DNS, as well as trigger the need for effective training. Organizations must also prioritize and budget 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. 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 against deliberate or unintentional malicious code injection or activation would be to limit product code deployment to certain hours of the day.

- Conducting exercises to test DNS services (e.g., "a day without the Internet"): Organizations must also develop and practice operational exercises to address technical vulnerabilities within the DNS in the event that a physical or logical attack degrades or disrupts any DNS servers. The Internet community does not know what the DNS server corruption threshold is that would render domain name translation incapacitated. The community can mitigate risk by increasing full-system modeling and simulation efforts to help identify possible courses of action in the event of an emergency and to predict possible outcomes. Additionally, these efforts should look to mitigate the current knowledge gaps regarding DNS vulnerability threshold levels and the security and stability impacts facing the Internet as new elements are added to the root zone.

After formulating the combined risk mitigation strategy, IT Sector partners concluded that full nation-wide implementation of the proposed mitigation steps above would reduce the national-level risk to *low likelihood* and *high consequence* (see Figure 6).

[15] NTIA released a Notice of Inquiry (NOI) asking for public comment on the testing and evaluation report and the commencement of the final stage of the DNSSEC deployment before it takes action. The NOI can be found at: http://www.ntia.doc.gov/frnotices/2010/FR_DNSSEC_Notice_06092010.pdf and the report can be found at: http://www.ntia.doc.gov/reports/2010/DNSSEC_05282010.pdf.

Figure 6: Effectiveness of Proposed Mitigation Strategy to Breakdown of Single, Interoperable, Global Internet



IT Sector partners agreed on the feasibility of implementing the proposed risk management strategy (see Table 5). IT Sector partners noted several key feasibility considerations, including:

- The Internet community is already implementing many of the proposed actions (in various stages of development/maturity), so barriers to implementation are low (for example, NTIA is currently implementing DNSSEC at the root); however, many of these proposals will require some time to implement;
- Legacy clients would face some technological barriers; however, since the focus of the risk management strategy is at the root-level, these technological issues would not be significant; the DNS community is currently discussing a proposed DNS-CERT capability, however, some members of the community are not in favor of the proposed concept. The final version of the proposed DNS-CERT capability may impact the feasibility of the proposed mitigation strategy, outlined in Table 5; and
- In terms of political feasibility, with less-developed areas coming online (e.g., Africa), the DNS community could expect increased criminal activity and spam (although this type of activity may increase in more-developed areas as well).

IT Sector partners noted that implementing the proposed risk management strategy would have positive effects on other critical functions, including *Provide Incident Management Capabilities*. IT Sector partners must analyze the risk mitigation strategy in greater detail to determine feasibility, implementation progress, and effectiveness measures related to this particular risk of concern.

Table 5: Feasibility of Proposed Mitigation Strategy to the Breakdown of Single, Interoperable, Global Internet

Feasibility Rating	Feasibility Factors	Description	Criteria
High	**Legal**	Statutes, regulation	The existing legal framework is favorable for implementing the proposed risk response.
High	**Organizational Compliance**	Best practices, organizational charters, corporate values	The implementation of the proposed risk response aligns closely with existing standards and best practices.
Medium	**Political**	Public confidence, privacy-related issues	Limited political issues may prohibit or inhibit implementing the risk response.
High	**Financial**	Cost, budget limitations	Normal market forces and existing business models will cover total average life-cycle costs to implement the risk response.
Low	**Time**	Reasonable schedule expectations	The implementation of the proposed risk response requires a relatively longer time frame (i.e., 24 months or longer for full implementation).
High	**Technology**	Ease of implementing existing technology or developing new technology	In the context of technological viability, the risk response is relatively easy to implement or develop.
High	**Market**	Market conditions, competition	The market conditions are favorable to implement the risk response.
High	**Compatibility**	Confidentiality, Integrity, and Availability after implementation	Minimal compatibility issues are associated with implementing the risk response.
High	**Cultural**	The alignment of IT Sector culture and the risk response	The IT Sector's cultural environment facilitates the risk response well.

3.3 Risk Response to Large Scale Attack on Infrastructure: Denial of Service (Manmade Deliberate)

3.3.1 Risk Overview

A number of large-scale attacks against the DNS infrastructure can lead to loss/denial-of-service. Potential attacks could be 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 the system would not necessarily paralyze the entire 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. IT Sector 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; 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 redirection, and other exploits of the DNS and routing protocols. Most non-nation-state actors lack the sophisticated resources that nation-states and other large organized cells might employ to conduct wide-scale coordinated attacks with cascading impacts. Cascading consequences could include denial or loss of service of Voice-over-Internet Protocol technologies, and electronic education and tracking systems; supply chain issues; disrupted or degraded electronic banking and shipment tracking; and credit trading. While the IT Sector SMEs did not discuss unintentional threats, an example is the unintentional loss of service resulting from a construction crew inadvertently severing underground communications cables. Such an incident would have limited impact to DNS services if it occurred in isolation; however, multiple cable cuts may impact the availability of DNS and Internet services over a wider area.[16]

In contrast to individual or group actors, many nation-states have significant resources and capabilities to conduct simultaneous 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; launching large-scale DDoS attacks; and building the capability for strategic cache poisoning. In addition, nation-states typically have more robust operational decision-making processes than individual actors, groups, or organizations, as well as more advanced capabilities to attack key cyber infrastructures to impact 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.

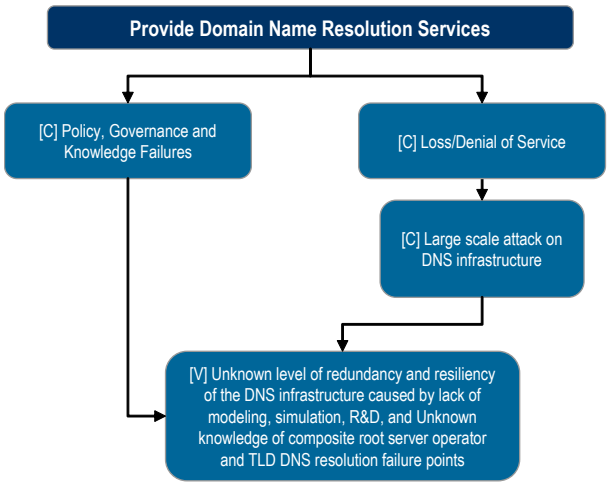
The first-order consequence of a manmade unintentional attack would most likely be a denial-of-service attack.[17] An unintentional modification of a portion of the DNS infrastructure, such as loading an outdated zone file or incorrectly modifying DNS records, would cause the DNS to distribute pointers to the wrong addresses. In this case, only those users who received replies from that DNS server would reach Internet destinations. 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.

ITSRA SMEs developed the following attack tree to scope the IT Sector's risk response strategy to a large scale denial of service attack on the DNS infrastructure.

[16] 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.

[17] 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.

Figure 7: Denial of Service by Large Scale Attack on Infrastructure (DNS 2a)



3.3.2 Risk Response

The ITSRA established that the national-level risk of a manmade deliberate large-scale attack on DNS infrastructure as being *low likelihood* and *high consequence* (see Figure 2). IT Sector partners agreed that the appropriate risk response to this particular risk of concern is a combined mitigation strategy, to include:

- Performing a gap analysis: One of the systemic problems regarding the Internet is the lack of aggregate knowledge of the entire Internet hierarchy (e.g., little information sharing between Internet Service Providers (ISP)/Registries/Registrars on threats, vulnerabilities, etc.). As such, the DNS community cannot accurately report on the DNS infrastructure's 'health'. Performing a gap analysis, as part of a system-wide global DNS risk analysis, will identify the major infrastructure entities that need to coordinate in the event of an attack.

- Adopting standards and best practices: The USG should focus on its DNS risk management efforts internally and adopt a set of standards or best practices to protect networks, and then work with international partners to adopt more globally-focused best practices.

- Developing a DNS dashboard: 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 operation centers to anticipate and protect DNS infrastructure from malware attacks. An integrated DNS dashboard (or confidence index) has the potential to provide real-time global monitoring of the DNS' entire "health" and could be used to measure DNS health from the user perspective. Developing a DNS dashboard would allow for increased transparency around DNS management and indicate whether the system is functioning as anticipated.

- Pursuing diplomatic and law enforcement responses: Depending on whether the attacker is known or unknown, one can employ different mitigation tactics (e.g., diplomatic apparatus for known state actors, etc.). However, if the source of the attack is unknown (e.g., a botnet), problems become more pronounced. If the attackers are known, diplomatic and law enforcement

responses should engage.[18] Such responses could be complemented by deploying or strengthening of kinetic and cyber deterrence capabilities.

- Improving emergency communications: In the event of an attack, critical entities must have a standardized, codified means of communicating with each other, particularly if Internet-based communications fail. Alternate communication mechanisms need to be deployed, or developed, to all key stakeholders. Solutions may include resorting to the most basic forms of communication and ensuring that all key players can participate in times of need (ham radio, etc.). The appropriate organizations should test and exercise regularly any improved communications mechanism.

In addition to the IT Sector partners' potential enhanced and future mitigation recommendations found in the ITSRA, other mitigation activities would include:

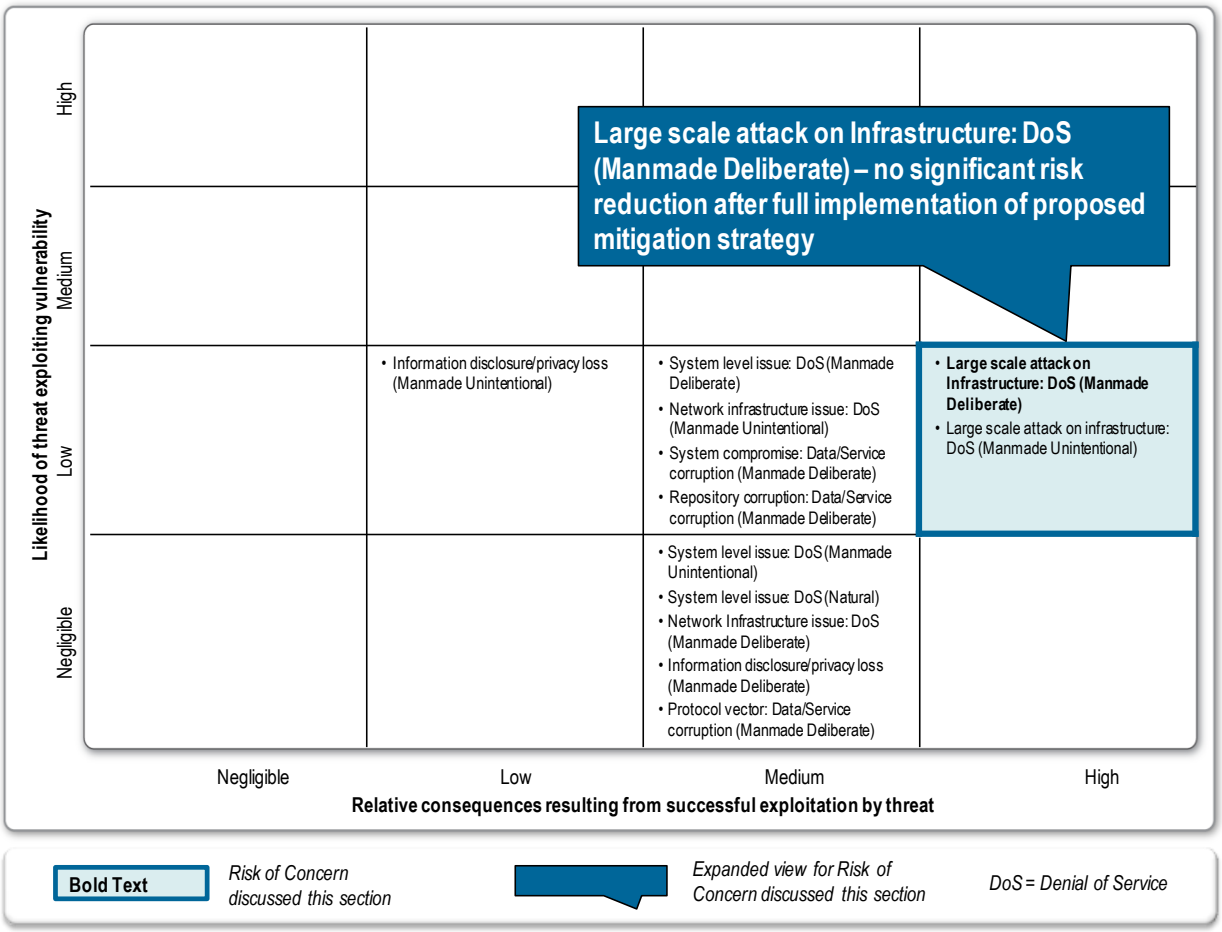
- Enhancing national-level modeling and simulation capabilities: To better understand and respond to pressures and impacts on the DNS, modeling and simulation of threats to the DNS is necessary. Such modeling and simulation should include IPv6, DNSSEC, IDN, and additional TLD impacts. National-level and multi-discipline modeling and simulation efforts could assist in developing a more unified effort to mitigate accidental risks. These efforts could encourage investment in 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 production code quality assurance, and load testing of any approved changes prior to "going live" can further mitigate risk. A possible mitigation strategy against deliberate or unintentional malicious code injection or activation would be to limit product code deployment to certain hours of the day.

- Conducting exercises to test DNS services (e.g., a day without the Internet): Organizations must develop and practice operational exercises to address technical vulnerabilities within the DNS in the event that a physical or logical attack degrades or disrupts any DNS servers. The Internet community does not know what the DNS server corruption threshold is that would render domain name translation incapacitated. The community can mitigate risk by increasing full-system modeling and simulation efforts to help identify possible courses of action in the event of an emergency and to predict possible outcomes. Additionally, these efforts should look to mitigate the current knowledge gaps regarding DNS vulnerability threshold levels and the security and stability impacts facing the Internet as new elements are added to the root zone.

After formulating the combined risk mitigation strategy, IT Sector partners concluded that, while implementing the proposed mitigation steps detailed above would strengthen the IT Sector's security posture and substantively reduce DNS risks, the national-level consequence rating would remain high and the national-level likelihood rating, while improved, would remain in the low range (see Figure 8).

[18] One such mechanism currently in place is the G8 24/7 network, which provides points of contact for investigations involving electronic evidence that require urgent assistance from foreign law enforcement. It is often technically necessary for investigators to move quickly to preserve electronic data and locate suspects, often by asking ISPs to assist by preserving data. Therefore, to enhance and supplement (but not replace) traditional methods of obtaining assistance, the G8 has created a network as a new mechanism to expedite contacts between participating nations or other autonomous law enforcement jurisdictions of a nation. Currently, over 45 member nations participate. For more information, see: http://www.oas.org/juridico/english/cyb20_network_en.pdf.

Figure 8: Effectiveness of Proposed Mitigation Strategy to Large Scale Attack on Infrastructure



IT Sector partners agreed that the proposed risk management strategy (see Table 6) is feasible to implement. IT Sector partners noted some key feasibility considerations, including:

- International legal, cultural, and political issues with both dashboard implementation and diplomatic and law enforcement response efforts may pose implementation challenges;
- The DNS community may not be fully receptive to having a DNS-CERT capability; and
- A DNS dashboard would be difficult to implement, given the varying complexity of DNS servers.

IT Sector partners noted that implementing the proposed risk management strategy would have positive effects on other critical functions, including *Provide Incident Management Capabilities*. However, the risk management strategy may encounter international political ramifications with diplomatic and law enforcement response efforts. IT Sector partners will need to analyze the risk mitigation strategy in greater detail to determine feasibility, implementation progress, and effectiveness measures related to this particular risk of concern.

Table 6: Feasibility of Proposed Mitigation Strategy to Large Scale Attack on Infrastructure

Feasibility Rating	Feasibility Factors	Description	Criteria
Medium	**Legal**	Statutes, regulation	The existing legal framework needs adaptation to implement the proposed risk response.
High	**Organizational Compliance**	Best practices, organizational charters, corporate values	The implementation of the proposed risk response aligns closely with existing standards and best practices.
Low	**Political**	Public confidence, privacy-related issues	Significant political issues may prohibit or inhibit risk response implementation.
High	**Financial**	Cost, budget limitations	Normal market forces and existing business models can cover total average life-cycle costs to implement the risk response.
Low	**Time**	Reasonable schedule expectations	The implementation of the proposed risk response requires a relatively longer time frame (i.e., 24 months or longer for full implementation).
Low	**Technology**	Ease of implementing existing technology or developing new technology	In the context of technological viability, the risk response is extremely difficult to implement or develop.
High	**Market**	Market conditions, competition	The market conditions are favorable to implement the risk response.
Low	**Compatibility**	Confidentiality, Integrity, and Availability after implementation	Significant compatibility issues are associated with implementing the risk response.
Medium	**Cultural**	The alignment of IT Sector culture and the risk response	The IT Sector's cultural environment moderately facilitates the risk response.