Provide Domain Name Resolution Services and Provide Internet Routing, Access, and Connection Services Critical Functions Risk Assessment

Information Technology Sector

May 2017

Homeland Security

INFORMATION TECHNOLOGY SECTOR COORDINATING COUNCIL

INFORMATION TECHNOLOGY GOVERNMENT COORDINATING COUNCIL

Table of Contents

Executive Summary

The Information Technology (IT) Sector provides services for the domain name system (DNS)[1] and Internet routing, access, and connection capabilities that underpin nearly all infrastructure supporting global Internet communications. In 2009, the IT Sector Coordinating Council (SCC) and its partners within the Department of Homeland Security (DHS) conducted a baseline risk assessment[2] of the IT Sector's critical functions, including DNS and Internet routing. Those findings, along with risk mitigation strategies developed in 2011[3] and 2013[4], have supported the IT Sector's ability to communicate risk both within the DNS and Internet routing communities, as well as to its many public and private stakeholders. Additionally, these efforts have been used to inform national-level responses to sector-wide queries. After the release of Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, in 2013, the IT Sector was able to draw from past reports to offer a coordinated and in-depth evaluation to inform the Cyber-Dependent Infrastructure Identification (CDII) effort. In response to ongoing changes in Internet policy environments, technologies, and protocols, the IT Sector determined that there was a need to update the risk profiles within the DNS and Internet Routing critical functions.

This updated assessment of the *Provide Domain Name Resolution Services* and *Provide Internet Routing, Access, and Connection Services Critical Functions Risk* describes how specific existing and emerging threats, technologies, and standards affect the risk profiles of the IT Sector's DNS and Internet routing critical functions. The assessment also discusses currently deployed mitigations and potential additional mitigations that might be needed to address the identified risks. Like previous IT Sector risk assessments, this risk assessment was conducted under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC) and is part of the National Infrastructure Protection Plan's (NIPP) implementation activities. As such, it was developed by subject matter experts from industry and government under the sponsorship of the IT SCC and IT Government Coordinating Council (GCC), with the DHS Office of Cybersecurity and Communications (CS&C) serving as the Sector-Specific Agency (SSA). These subject matter experts (SME) gathered during multiple sessions to assess risks to DNS and Internet routing infrastructure. The findings within this report are the culmination of their expertise and insights.

The risk assessment's results indicated that the likelihood of vulnerabilities in DNS and Internet routing infrastructure being exploited is moderate. As the number of Internet-connected devices continues to grow, so too will the risks to DNS and Internet routing infrastructure. The highly

---

[1] Mockapetris, Paul. *RFC#1034: Domain Names – Concepts and Facilities*. ISI, Nov. 1987. Web. 21 Jul. 2017 <https://tools.ietf.org/pdf/rfc1034.pdf>. *Original, but not inclusive definition.*

[2] Information Technology Sector. *IT Sector Baseline Risk Assessment*. Rep. IT Sector Risk Assessment and Mitigation working Group, Aug. 2009. Web. 31 Mar. 2017. <https://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf>.

[3] Information Technology Sector. *Information Technology Sector Risk Management Strategy for the Provide Domain Name Resolution Services Critical Function*. Rep. IT Sector Risk Assessment and Mitigation Working Group, June 2011. Web. 30 Mar. 2017. <http://www.it-scc.org/uploads/4/7/2/3/47232717/it-sector-risk-management-strategy-domain-name-resolution-services-june2011.pdf>.

[4] Information Technology Sector. *Information Technology Sector Provide Domain Name Resolution Services Critical Function Risk Profile Update*. Rep. IT Sector Risk Assessment and Mitigation Working Group, 2013. Print.

publicized 2016 Mirai botnet attack against a DNS service provider demonstrated the disrupting effects that a large-scale attack against DNS infrastructure can have on businesses relying on these types of services to conduct operations.[5] As such, this report provides industry and government stakeholders with a common understanding of the risks DNS and Internet routing operators face, and serves as a foundation for common action. The mitigations discussed within this report are not prescriptive, but they serve the important role of informing enterprise risk management strategies deployed by individual organizations.

For example, the results of this assessment can inform those utilizing the National Institute for Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*[6] (Framework) to assess their own organizational risks. Specifically, these results could be directly applied in the *Identify – Business Environment* and *Identify – Risk Assessment* Categories of the Framework. These DNS results may also inform other Framework Categories and Subcategories, depending on the organization. The contributors of this report hope that as the Framework gains traction, it will provide a means to help harmonize community-wide and enterprise-specific risk management efforts.

The process of creating this updated assessment consisted of three phases – (1) attack tree development; (2) threat, vulnerability, and consequence evaluation; and (3) risk analysis and reporting. SMEs from across the DNS and Internet routing communities (including operators and policy experts from both industry and government) participated in the assessment process.

Since the release of the initial 2009 IT Sector Baseline Risk Assessment (ITSRA) and subsequent updates, the Internet has continued to undergo changes that have affected the DNS risk profile. In many cases these changes have also affected the Internet routing risk profile due to the inextricable linkage between the two. These changes were highlighted and reflected in the assessment process and ultimately led to the identification of ten risk issues chosen for assessment. During scoping discussions, SMEs recognized three themes in the DNS and Internet routing critical functions:

- Dynamic Risk Environment
    - Implementation flaws found in commonly used open source libraries and collisions occurring from crossing administrative boundaries highlighted common process vulnerabilities.
    - Threat actor interest in route hijacking highlighted threats and the technologies (e.g., source address verification) used to mitigate them.
    - The increase in size and scope of distributed bot networks—such as the Mirai Internet of Things (IoT) botnet—has resulted in a massive increase in Distributed Denial of Service (DDoS) attacks with the largest attack of 2015 now being commonplace.

---

[5] Hilton, Scott. *Dyn Analysis Summary of Friday October 21 Attack,* October 26, 2016. Web. 03 Apr. 2017 <http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>

[6] National Institute for Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity,* February 12, 2014. Web. 21 JUL, 2017 <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

- Effects of Standards and Policies
    - Changes in domestic and global policies may affect organizations' ability to manage DNS infrastructure.
    - Consistently enforcing known mitigations to common vulnerabilities, such as Source Address Verification (SAV) to address Internet Protocol (IP) route spoofing.
    - Adoption of newer protocols, including IP version 6 (IPv6) and barriers to the deployment of the Domain Name System Security Extensions (DNSSEC), highlighted challenges that could introduce potential vulnerabilities upon implementation. As networks move to IPv6, the age-old model of leveraging the IP address itself will stop proving viable due to the increased size and complexity of the v6 networks.

- Growing Number of Devices Dependent on DNS Infrastructure and the Internet
    - The increasing number of IoT and mobile devices, many with minimal security features, connecting to the Internet and using DNS infrastructure have introduced new vulnerabilities and increased the attack surface an actor can use to compromise networks or other connected assets.
    - The increased use of shared cloud infrastructure has continued to trend upwards as more organizations move their content to infrastructure, which requires DNS to enable access.
    - The increased complexity of shared or outsourced infrastructure highlights how an organization’s supply chain introduces security considerations for DNS operators, requiring increasingly skilled staff.

These themes helped drive the identification of ten operational and strategic risk issues that provided the scope for the risk assessment. The assessment evaluated the impact that each risk issue could potentially have on the security and stability of DNS and Internet routing infrastructure. The results are derived from several factors, including existing knowledge obtained from historical attacks, as well as potential implications of future technology trends influencing the threat landscape against both DNS and Internet routing. Below is a brief description of each risk issue and related findings.

1. **Adoption of Software-Defined Networking (SDN):**

   As they become more common in Internet routing operations, the significance of securing SDN architectures will require network operators to remain aware of vulnerabilities and mitigations. Previously, SDN had only been implemented in a small subset of the operator community and did not pose a large-scale risk to the Internet Routing critical function. However, as the SDN industry continues to grow, the likelihood of an SDN vulnerability being exploited increases, as does the potential impact. Owners/operators should watch and evaluate the risk posed by the growing implementation of these technologies.

2. **Crossing Administrative Boundaries:**

Namespace collisions introduce vulnerabilities within DNS and Internet routing infrastructure and can lead to a loss of services. These collisions are also considered vulnerabilities themselves, but pose a relatively low risk to an organization's operations. There are two main threats that can exploit collisions: (1) the deliberate issuance of internal name certificates and (2) the unintentional exploitation through processing DNS search lists or name collisions. As the vulnerability poses a low risk to system operations within an organization and has been identified, an actor is unlikely to be able to exploit this vulnerability, and the impact would be minimal if the vulnerability is exploited.

3. **DNS Complexity Due to DNSSEC Implementation:**

   A loss of data and privacy, along with data or service corruption, is the most undesired consequence resulting from DNSSEC implementation. While the overall risk created from introducing DNSSEC into environments is low, challenges to DNSSEC deployment and ongoing maintenance introduce complexities in securing network infrastructure. Improper administration of DNSSEC can also lead to exploitations in the protocol itself, which can be used to flood a destination with data packets. As deployment increases and best practices for managing DNSSEC evolve, the risk rating will need to be reassessed against existing vulnerabilities.

4. **Incomplete IPv6 Transition:**

   The transition from IPv4 to IPv6 does not have inherent exploitation, but dual stack environments introduce additional complexity into a network, and compromised assets could cause degradation of DNS services. Many internal networks are employing transition-enabling methods (e.g., creating dual stack environments) or using network address translation. Misconfigurations associated with these methods could be exploited to cause a denial-of-service (DoS) attack, though the likelihood for this specific attack is low.

5. **Increased Attack Surfaces – Mobility and IoT:**

   The increasing number of Internet-connected devices accessing Internet content, including applications on those devices, continues to increase at a high rate. Large numbers of connected mobile and IoT devices create larger amounts of data and requires a greater number of routing activities. DNS and Internet routing infrastructure will be required to continue to increase in scale to meet demand for future levels of connectivity. Low levels of security combined with mobile and IoT environments provide attackers with new surfaces to launch attacks from or to directly attack. Exploitation of existing vulnerabilities of insecure IoT devices and the overall increase in Internet-enabled devices could increase the risk of degradation in DNS and Internet routing services. In addition, the devices themselves can be comprised and turned into attack vectors controlled by a malicious actor.

6. **Lack of SAV:**

   Lack of source address verification processes and technologies can lead to the degradation of DNS services. Because of the open nature of the DNS infrastructure, the

lack of source address verification could lead to DoS attacks where DNS resolvers and authoritative servers respond to packets regardless of the packets' origin. An actor or accident is relatively unlikely to exploit SAV vulnerabilities, but if those vulnerabilities are exploited, the consequences would degrade DNS services moderately.

7. **Route Injection and Hijacking:**

   Hijacking communication traffic or injecting new data into existing routing traffic could leave a system vulnerable to DoS or man-in-the-middle attacks. These attacks could result in the loss of data, damage to a company's reputation, and the long-term loss of consumer confidence. The likelihood of route injection or hijacking occurring is moderate, but its impacts would be minimal to the DNS and Internet routing critical functions as a whole.

8. **SSL Implementation Errors:**

   The installation of new software and hardware, especially in open recursive resolvers and authoritative servers, could introduce vulnerabilities due to misconfigurations or incompatibility with the existing system. The impacts of implementation errors being exploited are likely to lead to some mission degradation, but the likelihood of the vulnerabilities associated with implementation errors being exploited is low, intentionally or otherwise. Mitigations already in place temper the likelihood of these flaws of being exploited, but the sector's ability to provide domain resolution services would be greatly affected if a threat actor can exploit these vulnerabilities.

9. **Stewardship of the Internet's Technical Identifier Resources:**

   SMEs recognized that ongoing policy activities in the DNS and Internet stewardship environments may have implications on the IT Sector's risk profile. The assessment recognizes the importance of stewardship on the IT Sector's provision of DNS and had the desire to identify relevant aspects of the topic. However, SMEs would like to evaluate the topic fully in the future once the policy and technical landscapes are more clearly defined.

10. **Supply Chain Risk to DNS:**

    DNS infrastructure hardware has commonly been replaced by software architectures that can easily be deployed in a dynamic network environment. However, as more of these services are used by members of an organization's enterprise and supply chain, additional risks can be introduced into managing Internet communications. Technical complexity of the software used by the DNS functions can result in several points of failure that could lead to cascading effects capable of disrupting Internet routing and DNS access. Supply chain vulnerabilities are often considered in any risk assessment, and Internet routing and DNS services are no different.

These ten issues do not address all risks faced by IT Sector stakeholders. They do, however, provide a snapshot of the more prominent risks facing critical infrastructure owners and

operators. These risks were identified by SMEs in a collaborative and iterative process and allowed for priority risks to be highlighted.

The assessment also identified risk mitigations that are observed across the operator community who were actively implementing mitigations to address the vulnerabilities discussed in this report. These mitigations are considered adoptable by other operators trying to increase security across high-risk areas specific to their own organizations. Given the interconnected nature of DNS and Internet routing infrastructure, several of the mitigations discussed are applicable across many of the risk issues. DNS and Internet routing operators of all sizes employ common mitigation practices to address people, process, and technology vulnerabilities within their environment. The following mitigations were identified by SMEs as those most commonly deployed by owner/operators to mitigate risks of concern.

People: Practices in place to mitigate vulnerabilities that are introduced by the personnel managing DNS and Internet Routing infrastructure include:

- Operators implement proper education and training programs to ensure staff are capable of using new technologies to operate DNS and Internet routing infrastructure and protect the infrastructure against new common threats.

- Employee monitoring and supervision to ensure that appropriate administrative privileges and access levels are in place.

- DNS operations rely on a limited number of employees. Auditing employee actions, usually through automated technologies, can reduce repeated mistakes or single points of failure.

Process: Practices in place to mitigate vulnerabilities existing within common organizational procedures supporting DNS and internet routing operations include:

- Operators deploy change management and configuration management practices in their organizations, particularly when changes are made to hardware or software within networks.

- Mature incident response plans that allow operators to respond quickly to changes in the risk environment or actual attacks.

- Operators use processes or technologies to monitor threats and resources and filter incoming traffic to maintain situational awareness of networks.

Technology: Practices in place to mitigate vulnerabilities that arise from technologies (i.e., hardware and software) and the introduction of new technologies into existing environments include:

- Operators use robust modeling and simulation to test new technologies, sometimes through red zone trials, before fully introducing them.

- Operators use rate-limiting to control the rate of traffic handled by infrastructure.

- Following industry best practices to have redundant infrastructure available that handles the most critical services used across network operations, including but not limited to secure coding, IP address configuration, protocol and service deployment such as Border Gateway Protocol (BGP), and DNSSEC configuration. All of these technologies together have increased the complexity of adversary profiles, threats, vulnerabilities, and mitigations, making redundant and self-healing infrastructure critical to successfully supporting operations.

This is not an exhaustive list of existing and future mitigations. However, it does provide an understanding of some common approaches taken to address risks to the DNS and Internet routing infrastructure.

1 Background and Context

1.1. IT Sector Baseline Risk Assessment

In August 2009, the DHS and the IT SCC published the ITSRA. This report identified six critical functions in the IT Sector; analyzed the possible, threats, vulnerabilities, and consequences to those functions from deliberate attacks, unintentional accidents, and natural events; and identified strategies to mitigate and manage the risks to the sectors. The six IT sector critical functions and their capabilities are illustrated in Figure 1.

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 Doman 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 1: Key IT Sector Functions

The ITSRA was developed as a collaborative effort by representatives from DHS, other Federal Government agencies, the Department of Defense, private industry, and other organizations involved in Internet operations, governance, and standards development. The objective was to base the ITSRA's conclusions and recommendations through methodical processes that leveraged the real-world experience of SMEs.

The original 2009 ITSRA included an examination of the DNS and Internet routing critical functions. For the *Provide Domain Name Resolution Services* critical function, SMEs provided an overview of DNS infrastructure and technology, including the hierarchy of name servers and

the effect of DNS protocols on Internet communications. SMEs identified four high-level consequences that would affect the IT Sector's ability to provide DNS and ultimately, two risks that were of greatest concern to the IT Sector, including:

1. Breakdown of a single interoperable Internet through a manmade attack, and resulting failure of governance policy; and
2. Large-scale manmade DoS attack on the DNS infrastructure.

SMEs also provided an overview of the *Provide Internet Routing, Access and Connection Services* critical function, including the distributed nature of Internet facilities, the adaptability of packet switching, and the role that Internet service providers (ISP) have in the process. They identified three high-level consequences that would affect the IT Sector's ability to provide Internet routing:

1. A partial or complete loss of routing capabilities, either locally, regionally, or across large parts of the world, caused by deliberate or unintentional actions;
2. Natural disasters or manmade incidents that could impair the operation of concentrated routing facilities; and
3. Ineffective or impaired responses to restoring routing operations after an outage or an incident.

The risk of greatest concern to the IT Sector's risk profile was identified as a partial or complete loss of routing capabilities through a manmade deliberate attack on the Internet routing infrastructure.

1.2. 2017 DNS Risk Profile Update

While none of the IT Sector critical functions has remained static since the ITSRA was published, both the DNS function and the related Internet routing function have undergone some degree of evolutionary change, including: DNS and routing security becoming more pressing concerns for operators and users; significant deployment of IPv6 addressing by network operators; greater number of DoS attacks on ISPs, DNS operators, and network providers with increased sophistication[7]; and nation states intent on exercising control over Internet access blocking DNS services or cutting off outside access entirely.[8] As such, representatives from the IT SCC; IT GCC; IT Information Sharing and Analysis Center; and other government, industry, and academic organizations agreed to update the DNS and routing assessment.

[7] DDOS takes down Cirrus Communications: Australian fixed wireless provider loses half its network for a day or so: http://www.theregister.co.uk/2014/07/30/ddos_takes_down_cirrus_communications/.
[8] Government begins to shut down Internet and television in Ukraine: http://www.intellihub.com/government-begins-shut-internet-television-ukraine/ ; Iraq Shut Down Internet Access In 5 Provinces; http://www.businessinsider.com/iraq-internet-shutdown-2014-6.

2 Scope, Process, and Audience

2.1. Assessment Scope

IT Sector stakeholders continue to recognize the reliance on the DNS protocol for Internet communications as a critical element of IT infrastructure. In addition, the 2013 EO 13636, *Improving Critical Infrastructure Cybersecurity*, CDII effort outlined threats to the Border Gateway Protocol (BGP) and the resulting implications of an impairment of BGP as an area warranting greater study. DNS and Internet routing partners were consulted to identify and recruit a group of knowledgeable SMEs who could speak to the threats, vulnerabilities, and consequences that comprise risks to the DNS and Internet routing critical functions. Government and industry SMEs collaborated to explore the anticipated technical and policy implications of an incident or attack impacting DNS and Internet routing infrastructure and assess the likelihood of an incident or attack given today's threat environment and risk responses.

Considering the results of the ITSRA, along with changes to both DNS and Internet routing environments, SMEs participated in three facilitated scoping sessions and identified ten risk topics to evaluate through the assessment. The ten topics assessed in this study are presented in alphabetical order below and in this report:

1. Adoption of SDN;
2. Crossing Administrative Boundaries;
3. DNS Complexity Due to DNSSEC Implementation;
4. Incomplete IPv6 Transition;
5. Increased Attack Surfaces - Mobility and the IoT;
6. Lack of SAV;
7. Route Injection and Hijacking;
8. SSL Implementation Errors;
9. Stewardship of the Internet's Technical Identifier Resources; and
10. Supply Chain Risk to DNS.

Participating SMEs made these observations, and in so doing, examined how each of these topics affected and have been affected by the evolution of the Internet, especially as it pertains to the ability of the IT Sector to provide DNS and Internet routing functions. They also discussed what government, private industry, and other organizations could do or are already doing to enhance the reliability, stability, and security of the Internet and mitigate potential threats and vulnerabilities to providing the functions. The findings within this report reflect the gathered SMEs' assessment of risks to the DNS and Internet routing functions as they stand at this time.

2.2. Attack Tree Evaluation Process

This update to the DNS risk assessment used the same evaluation process that was deployed in the original ITSRA and other updates. First, SMEs identified national level consequences that could result from a failure in the critical function. Then, the SMEs developed attack tree scenarios to map out how such consequences could be achieved through an attack on the critical

function. Attack trees offer a logical argument chain that depicts how a series of events could lead to an undesired outcome. By using attack trees as a common framework, participating SMEs identified undesired consequences; vulnerabilities that could be exploited to cause the undesired consequence; and threats that could exploit the vulnerabilities. The criteria used for rating vulnerabilities and consequences are depicted in Figure 2.

Criteria	Definition	Rating
Mission is Severely Degraded	End Users are unable to meet foundational and basic mission requirements	High
Some Mission degradation will occur	End Users are able to meet the foundational and basic mission requirements but are unable to complete their missions in their entirety	Medium
Only slight effect on mission	End Users are able to complete their missions but operations have been affected	Low
No identifiable effect on mission	End Users are able to fully complete their missions and continue operations	Negligible

Figure 2: Vulnerability and Consequence Rating Criteria

In conducting this risk assessment, SMEs updated relevant DNS and Internet routing attack trees created during the ITSRA to better characterize and evaluate risks across each of the ten topic areas. The attack trees illustrate the scope of the assessment for each topic. In addition, they form the basis of each risk description and the evaluation of risk to the DNS and Internet routing critical functions.

Within each attack tree for each topic, SMEs also evaluated two different types of threat categories where appropriate, including:

- Manmade deliberate: The manmade deliberate threat component focuses on incidents that are 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; and

- Manmade unintentional: The manmade unintentional threat component focuses on incidents that are 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.

2.3. Audience

The risk assessment process and this report are the DNS and Internet routing community's opportunity to educate the following audiences on the risks they face and the actions that can be taken to mitigate these risks:

- Decision-makers in DNS and Internet routing owner/operator organizations[9]; and
- Decision-makers and policy developers involved in Internet governance and policy.

Some risk analysis and risk mitigation recommendations may be more relevant and useful to DNS and Internet routing owners and operators than others. In addition, some analyses focus on emerging technologies that may not currently have a significant impact on the IT Sector's risk profile, but their increased adoption could affect the risk profile in the future.

[9] Owners and operators may include organizations such as domain name registrars, ISPs, Web hosting providers, domestic backbone carriers, and Internet backbone providers.

2.1. SDN: Background

It may be possible to compromise new SDN network architecture that separates the control plane from the data plane, decoupling them from underlying distributed hardware. Malicious actors can redirect traffic to carry out a man-in-the-middle attack and direct packets to compromised nodes.[10]

SDNs are new architectures that separate the control plane from the data plane in Internet routing operations. This creates centralized network intelligence and state information functions, decoupling them from underlying distributed hardware. Separating control from the hardware can create vulnerabilities. SDN represents a paradigm shift in how organizations deploy virtual infrastructure used to operate networks and network functions. Being able to reconfigure how networks function through lines of software code rather than the arduous process or reconfiguring hardware is a trend fueled by cost and time savings and is expected to continue to increase in the future.

To evaluate the threats, vulnerabilities, and consequences to the *Provide Internet Routing, Access, and Connection Services* critical function, SMEs determined the increasing use of SDN could potentially cause one of the undesired consequences identified in the ITSRA: Partial or complete loss of routing functions and support services. Although SDN architectures centralize important network processes, they may introduce vulnerabilities by removing the process from the underlying hardware in the routing process. These vulnerabilities can impact connectivity to the routing network's Interdomain or backbone. Some backbone networks are large enough that smaller routing networks depend on them, creating a cascading effect across the routing hierarchy. SMEs identified attacks on control plane communications and forged or fake traffic flows as the most likely actions of deliberate actors wishing to affect routing functions. Figure 3 describes the threat [T] and vulnerability [V] SMEs identified that could lead to undesired consequences [C] within the topic.

[10] Weinberg, Neil. "Is SDN your next security nightmare?" Networkworld. 30 March 2014. http://www.networkworld.com/article/2174811/lan-wan/is-sdn-your-next-security-nightmare-.html.

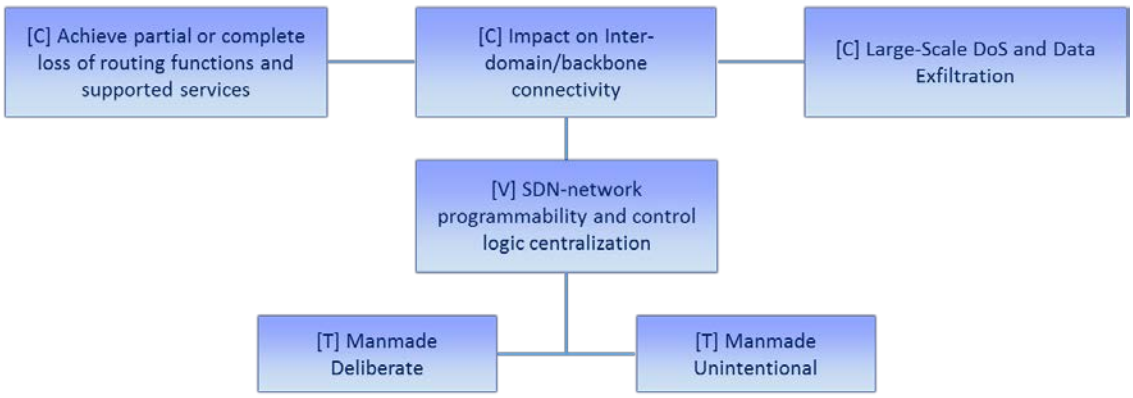

Figure 3: SDN Attack Tree Summary

Malicious actors or faulty devices could trigger forged traffic flows creating an attack on Open Flow switches and controller resources. Once attacked, actors can then target Ternary Content Addressable Memory (TCAM), exhausting data capabilities and creating a partial or complete loss of routing functions and services. Through forged traffic flows, actors can also target the implementation of Transport Layer Security (TLS) and Secure Sockets Layer (SSL) communications protocols between the routing controllers and the end-user devices. These protocols would be vulnerable to man-in-the-middle attacks, allowing attackers to read and manipulate traffic.

By signing traffic to improve service availability, operators are able to ensure Open Flow switches and controller resources are not compromised. Signing DNS traffic is not a part of legacy DNS operations and this process, along with SDN, may become increasingly implemented and important in the provision of DNS and Internet routing services.

2.2. SDN: Risk Assessment

SMEs recognized the significance of SDN architectures as SDN become more common in Internet routing operations. SMEs assessed risk as it currently exists, particularly the ways in which malicious actors could exploit existing vulnerabilities, and recognize the need to evaluate the risk posed by the growing implementation of SDNs in future updates. Undesired consequences associated with SDN include large-scale DoS attacks, traffic redirection, and data extraction. Inadequate implementation of SDN technologies could also lead to a loss in connectivity. While operators and end-users would most likely be affected through a lack of routing functions, ISPs could also be affected through a loss of network control.

Personnel vulnerabilities, most likely associated with SDN implementation, involve inadequate administrative experience with the new technology. A general lack of standards and lack of best practices with the technology in the routing environment may be compounded through inadequate use of best practices with associated mitigations (e.g., DNSSEC) and protocols (e.g., SSL). The introduction of SDN in operator processes can lead to inadequate diversity or redundancy in networks and improper asset management of systems and platforms. Because of the relative newness of the technology, a lack of certification and accreditation could also make the system vulnerable. The introduction of the technology would be new to the implementing organization which may cause owners and operators to find their current quality control and

auditing processes lacking. The most significant technology vulnerability would involve interoperability issues between older DNS networks and newer SDN architectures.

SMEs identified the most common malicious actors to be vandals or hacktivists looking to impact routing capabilities, including large-scale DoS attacks and data extraction. With more Internet application providers moving to SDN to manage their internal networks, criminal or state-sponsored attacks may occur in an attempt to obtain private information. The threat actors' main goal would be to open a routing channel to collect and extract data on an ongoing basis for an extended period. Actors would then be able to extract data from both the control plane (including logical data) and from the data plane (including actual user data). Through man-in-the-middle attacks, actors could manipulate or redirect traffic and create a significant loss in routing functionality.

In addition to DNS or Internet routing operators, large-scale content providers are also using SDN architectures to manage their systems or to access content. However, while the consequences of an attack on many content providers are reasonably low, content providers with many users or valuable data may be tempting targets for SDN exploitation.

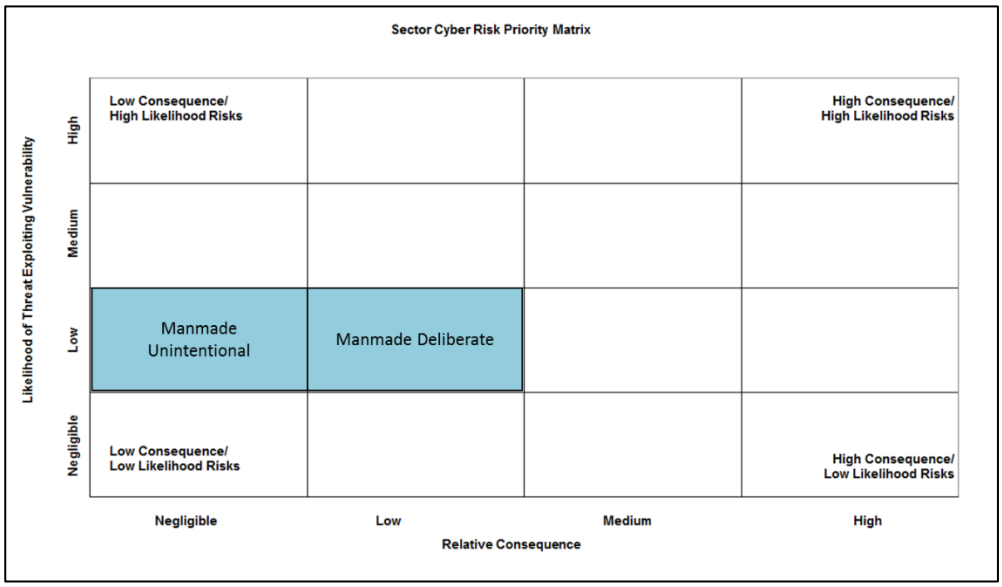

Figure 4: SDN Risks to the Provide Internet Routing, Access and Connection Services Function

2.3. SDN: Risk Mitigations and Recommendations

People, process, and technologies associated with SDN vulnerabilities are currently being mitigated with a variety of responses.

To mitigate vulnerabilities introduced by the people involved with SDN operations, owners and operators use:

- Regular training programs on SDN technology;
- Supervision of staff and assets providing SDN; and
- Security policy compliance audits against security standards.

To mitigate vulnerabilities introduced by the processes involved with SDN operations, owners and operators employ:

- Quality control;
- Auditing;
- Certification; and
- Asset management programs.

To mitigate vulnerabilities introduced by the technologies involved with SDN operations, owners and operators employ:

- Stay current with proper Patch management;
- Develop deployment best practices and actionable lessons learned; and
- Regular Penetration testing to identify misconfigurations or vulnerabilities.

Ultimately, by using diverse, redundant networks and proper incident response planning, owners and operators mitigate against these topic-specific attacks and help manage against the cascading effects of successful incidents. Network operators, standards development organizations, and government agencies can play roles in promoting and supporting SDN through several actions, including securing SDN software to industry best practices, conducting periodic security audits and ensuring security patch releases are installed.

3 Crossing Administrative Boundaries

3.1. Crossing Administrative Boundaries: Background

DNS resolution crosses administrative boundaries between internal sub-domains and Top Level Domains (TLD), and trust may be imputed into DNS where it should not reside. When crossing administrative boundaries, routing errors and name collisions can occur resulting in undesired route redirection and loss of service.

SMEs identified the loss or DoS of the critical function as a main undesired consequence associated with crossing administrative boundaries. Figure 5 illustrates high-level vulnerabilities and threats identified by SMEs that could lead to the undesired consequence within this topic. Network infrastructure vulnerability could be exploited through a routing error, incorrect name resolution, or name collision across boundaries. They also identified two main threats as having potential access to these vulnerabilities. The first is a deliberate threat coming from the issuance of internal name certificates. The second is the unintentional exploitation through processing DNS search lists or name collisions.

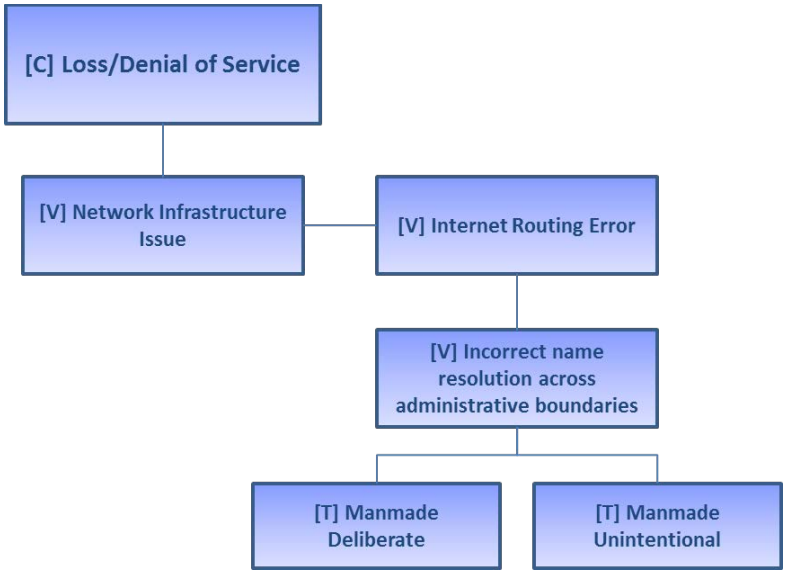

Figure 5: Crossing Administrative Boundaries Attack Tree Summary

Domain names that lack consistency across boundaries lead to namespace collisions. Such name collisions can provide incorrect lookup results and opportunities for traffic redirection using internal host names. DNS namespace collisions contribute to security and availability issues. Organizations often have internal sub-domains that can cause confusion when presented to the DNS resolver, creating the opportunity for route injection. In a few limited cases with some new TLDs available for use, malicious actors could feasibly spoof addresses on private networks to

redirect traffic away from a user's intended address.[11] As new TLDs are introduced into the DNS, it is important that networks are properly managed to address this issue. It is anticipated that name collisions with internal sub-domains will continue to occur, but will not increase in number. In fact, they will decrease in time as users correct their internal systems.

3.2. Crossing Administrative Boundaries: Risk Assessment

Undesired consequences that could result from traffic redirection and DoS attacks include a loss of or damage to data, financial assets, or reputation. The introduction of new technologies can force namespace collisions, cause a loss of corporate resources, or open users up to identity theft. Most threats in this category would be limited to the specific DNS zone that was altered, reducing the overall vulnerability of the DNS as a whole and the overall consequences associated with crossing administrative boundaries.

Potential personnel vulnerabilities ranged from lack of expertise and adherence to best practices to new registry operators of TLDs. SMEs also identified vulnerabilities in processes, including inadequate quality control and auditing, as well as a lack of proven methods and practices, specifically around namespace collisions. Technology vulnerabilities were attributed to the openness of the technology and a lack of security in the configuration of local systems. Legacy hardware, specifically routers, contributes to physical vulnerabilities and the potential free access to the hardware by authorized employee threat actors.

During the assessment, SMEs identified deliberate threats from organized crime, nation states, hacktivists, and rogue employees with the objective of financial or proprietary informational gain. To achieve their goals, threat actors could use DoS attacks, interrupt services, and redirect traffic. Due to the resources necessary to carry out an attack, the threat would likely come from a formally organized team with a good understanding of the underlying technology.

In discussing logical access, SMEs determined that the threat actor would need to have insider access in order to exploit potential vulnerabilities. A nation state or organized crime group would need to gain logical access with appropriate credentials to get into the system. A rogue employee would need to have or obtain the necessary privileges to exploit the system as well. With the addition of IoT devices becoming more prevalent in organizations, often times with weak security features, an insider could potentially compromise one of these IoT devices capable of communicating directly with DNS infrastructure in order to discover additional network characteristics that could be exploited, without needing direct access to the DNS infrastructure itself.

An infrastructure operator or network administrator with authorized logical access and significant autonomy could become an unintentional threat actor. SMEs determined that the operation of the function would be the actor's primary job, therefore there is potential that distractions or a disregard for established policies could lead to careless errors. A lack of training could also lead to unintentional mistakes. SMEs determined an unintentional threat was

[11] Jackson, Brian. "New domains carry risk of 'name collision' attacks: OpenDNS." ITbusiness.ca. 23 April 2014. http://www.itbusiness.ca/news/new-domains-carry-risk-of-name-collision-attacks-opendns/48271.

more likely to occur than a deliberate threat, even though the exploitable vulnerabilities remain the same.

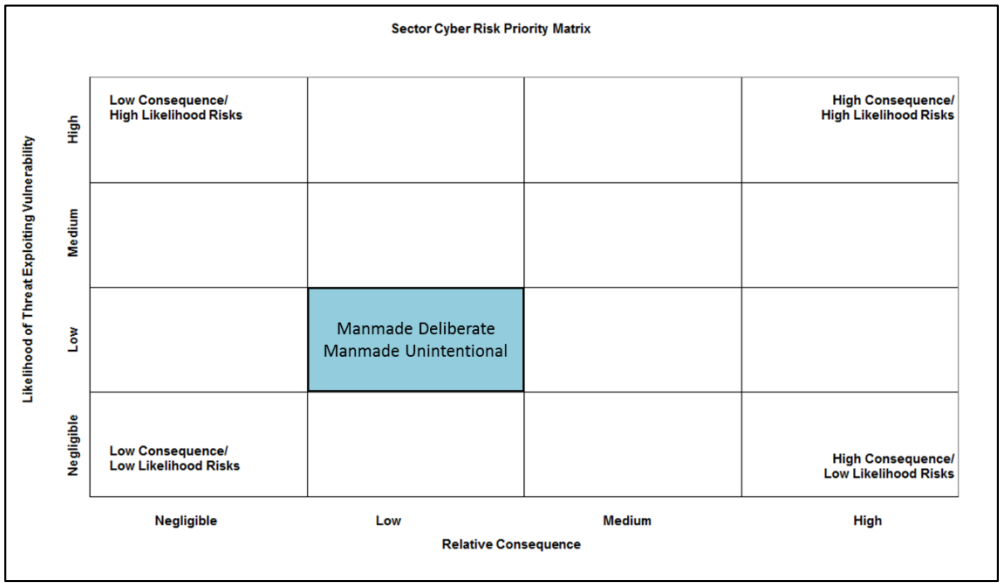

Figure 6: Crossing Administrative Boundaries Risks to the *Provide Domain Name Resolution Services* Function

3.3. Crossing Administrative Boundaries: Mitigations and Recommendations

Organizations are currently using a variety of responses to mitigate people, process, and technology vulnerabilities associated with crossing administrative boundaries.

To mitigate vulnerabilities introduced by the people involved with crossing administrative boundaries, owners and operators use:

- Education and training;
- Participation in the industry community;
- Recognized policies and standards; and
- Monitoring, auditing, and oversight of employees.

To mitigate vulnerabilities introduced by the processes involved with crossing administrative boundaries, owners and operators employ:

- Incident response capabilities;
- Change management practices to reflect changes; and
- Configuration management practices maintained and followed.

To mitigate vulnerabilities introduced by the technologies involved with crossing administrative boundaries, owners and operators employ:

- Updated firmware and/or hardware;
- Quality assurance;
- Modeling and simulation techniques;

- Red zone delegation trials to see how technologies, and the environments they operate in, interact with their entry within an individual entity's system; and
- Consider or deploy a DNS Firewall, also known as a Response Policy Zone to intercept and contain the scope of certain query names or domains.

Network operators, standards development organizations, and government agencies can play roles in guarding against domain name collisions through several actions, including:

- Auditing their networks (both internal and public facing) to ensure that systems do not use references to TLDs that could potentially collide in the namespace (such as ".prod", ".corp"); and
- Deploying DNSSEC (both authoritative servers and validation).

4 DNS Complexity Due to DNSSEC Implementation

4.1. DNS Complexity Due to DNSSEC Implementation: Background

DNSSEC is the deployment of a set of extensions to DNS protected zones that authenticate DNS data and integrity. DNSSEC implementation also requires cryptographic key management and has resulted in the creation of larger packets during DNS queries. These larger packets could facilitate DNS amplification and DoS attacks.[12]

DNSSEC is a means to ensure that responses from DNS servers are both authentic and non-reputable, and it can mitigate certain types of DNS redirection and hijacking attacks. Entities have developed procedures and technology for implementing DNSSEC, but the level of DNSSEC implementation remains low. As such, key management is the focus in this assessment.

DNSSEC is designed to protect DNS records with a cryptographic signature, in order to ensure that the response is from the true originating server. Unfortunately, there is a double-edged sword with DNSSEC, notably that the responses can often be significantly larger than the original DNS record itself. As seen in DDoS attacks using DNS amplification, large DNS records are a very effective way to get a small amount of spoofed traffic to generate a very large amount of response traffic, with possible amplification levels of 100x or greater. In this way, an attacker with 10Gbps of bandwidth can generate a Terabytes per second attack "response" aimed at a spoofed target. The DNS community will have to continue to monitor amplification attacks, and collaborate with network security engineers to reduce the attack footprint of open DNS resolvers where possible.

Undesired consequences associated with DNSSEC implementation include information disclosure, privacy loss, data corruption, and service degradation. Figure 7 describes the vulnerabilities and threats that SMEs determined could lead to undesired consequences within the topic. Vulnerabilities were identified across three tiers of exploitation. Inappropriate key generation and storage or an unsuccessful key rollover can lead to inadequate DNSSEC key management. The inadequate management then leads to an increase in the "brittleness" or limited resiliency of DNS, resulting in undesired consequences. Additionally, manmade deliberate or unintentional threat actors can exploit both vulnerabilities.

[12] Lindsay, Greg. "DNSSEC and DNS amplification attacks." Microsoft Security TechCenter. 23 April 2012. http://technet.microsoft.com/en-us/security/hh972393.aspx.

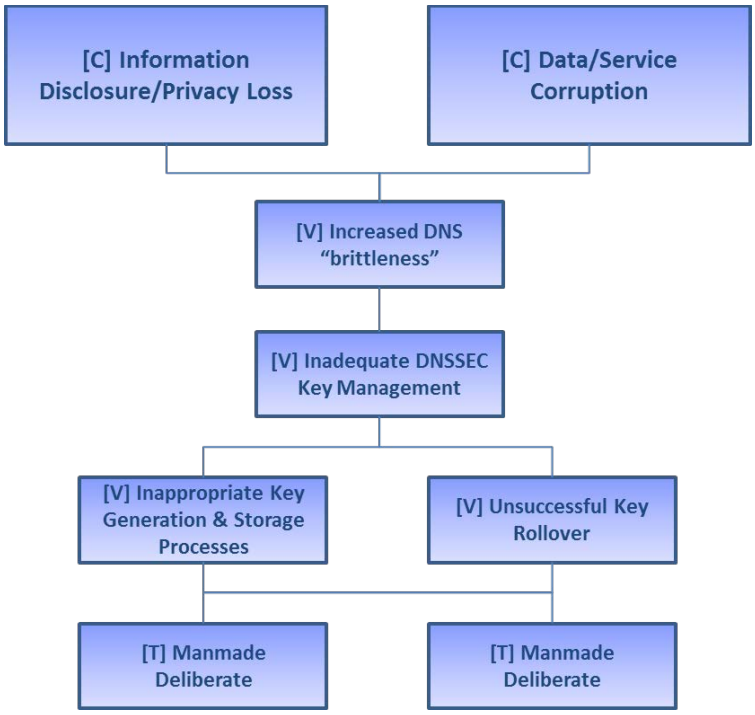

Figure 7: DNSSEC Complexity Due to DNSSEC Implementation Attack Tree Summary

The complexity arising from the implementation of DNSSEC causes possible risk areas, including the loss of faith in DNS management, traffic redirection, and DoS. However, SMEs noted that there is an inherent trust in DNS because of necessity. The top level of the DNS hierarchy, the "root" zone, serves as an entry point to answer queries. Figure 8 depicts the hierarchy that exists between the root zone and Top and Lower Level Domains.

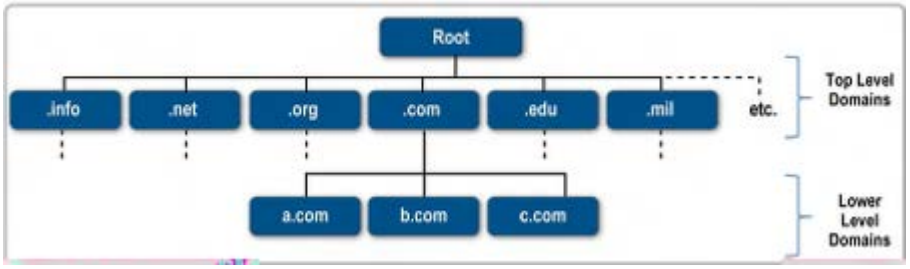

Figure 8: DNS Hierarchy

4.2. DNS Complexity Due to DNSSEC Implementation: Risk Assessment

Attacks or accidents associated with DNSSEC implementation are likely to impact the availability and confidentiality of information. An attack during the look-up phase of a DNS query has the ability to redirect traffic to malicious websites resulting in website outages, loss of data confidentiality, and communications capabilities. DNSSEC authenticates the origin of the information as the authoritative name server responds through the ISP caching resolver.

From a personnel perspective, SMEs identified several potential vulnerabilities, including: lack of technical management expertise; lack of organizational discipline to maintain knowledgeable staff; varying levels of expertise among third party DNS managers; and segmented expertise within DNSSEC. SMEs also identified inadequate adherence configuration management, auditing, and tools as process-oriented vulnerabilities. The lack of an end-to-end solution for stub resolvers (i.e., simple, non-iterative resolvers) and the costs to maintain and upgrade infrastructure were identified as technology-related vulnerabilities. Additionally, SMEs identified several risk responses already in place to mitigate against these vulnerabilities. These risk responses include training, implementation of automated tools, implementation of current best practices, and firmware upgrades.

SMEs identified nation states, organized crime, and rogue employees as potential deliberate threat actors. Nation states are the most likely to have extensive financial resources and technical capabilities. Organized crime members and rogue employees are likely to have fewer financial and technical resources, but their technical capabilities are likely to remain high. Deliberate threat actors exploiting DNSSEC vulnerabilities intend to steal information for political and financial gain or to degrade the credibility of entities managing important or highlight visible domains. SMEs also identified poorly trained employees and third-party contractors as potential unintentional threat actors. In order to carry out an attack or accidentally exploit a vulnerability, logical access would be required. Such access is likely to be obtained through an authorized actor, either a current inside employee or an outside actor with temporary but legitimate credentials.

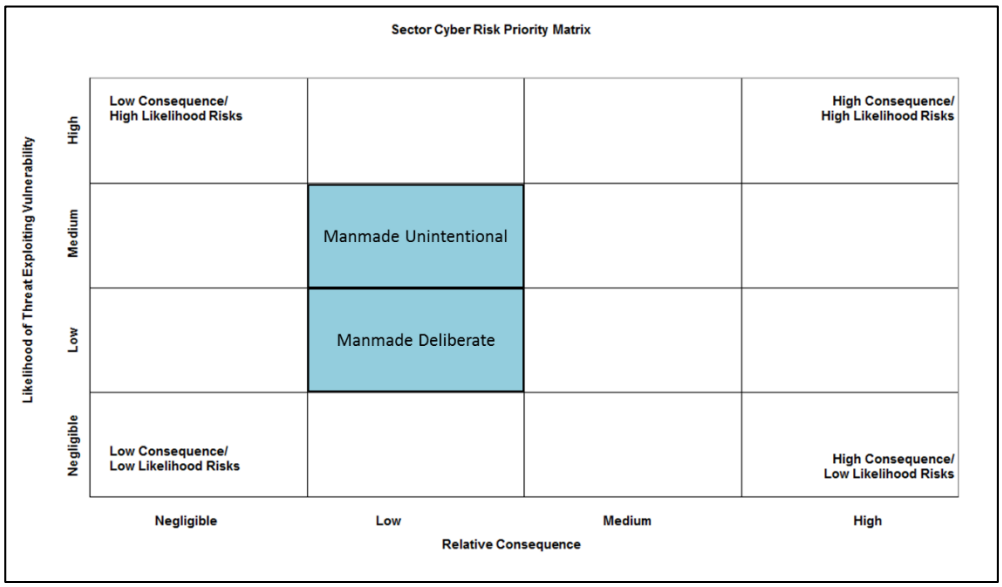

Figure 9 DNS Complexity Due to DNSSEC Implementation risks to the Provide Domain Name Resolution Services Function

4.3. DNS Complexity Due to DNSSEC Implementation: Mitigations and Recommendations

People, process, and technology vulnerabilities associated with the implementation of DNSSEC are currently mitigated with a variety of responses.

To mitigate vulnerabilities introduced by the people involved with DNSSEC implementation, owners and operators use:

- Education and training of network admin staff;
- Recognized policies and standards followed and updated;
- Automated tools deployed to assist network security staff; and
- Employee monitoring, auditing, and oversight to ensure compliance.

To mitigate vulnerabilities introduced by the processes involved with DNSSEC implementation, owners and operators use:

- Regular Auditing;
- Change management practices developed and followed;
- Configuration management practices; and
- Consistent implementation of best deployment practices.

To mitigate vulnerabilities introduced by the technologies involved with DNSSEC implementation, owners and operators use:

- Rate limiting, or “throttling” of the number of outgoing DNS requests;
- Quality assurance;
- Modeling and simulation techniques; and
- Best current practices on DNSSEC implementation.

Network operators, standards development organizations, and government agencies can play roles in promoting and supporting DNSSEC implementation through several actions, including:

- Promoting the use of DNSSEC through contract requirements; and
- Actively auditing and monitoring zones for DNSSEC errors.

5 Incomplete IPv6 Transition

5.1. Incomplete IPv6 Transition: Background

Security researchers demonstrated how they could use a man-in-the-middle attack to intercept and reroute traffic by installing a router onto an IPv4 network to receive IPv6 packets. While the threat actor would need physical access to a target network to install the router in this scenario, it highlights one method that can exploit IPv4 and IPv6 network settings.[13] *While IPv6 is available nearly ubiquitously, the transition from IPv4 is incomplete, and may stay so for a while, leading to a "dual stack" environment requiring more resources to administer.*

The next generation of IPv6 was designed to replace the limited number of IP addresses available in the existing IPv4 addressing scheme. Many organizations, including the Federal Government, began transitioning communications infrastructure to operate in a way that's compatible with both IPv4 and IPv6 addressing schemes, leaving a much more complicated "dual stack" environment for network operators to manage. Many organizations do not need to migrate to IPv6, leaving the transition incomplete, adding additional risks to consider for DNS and Internet Routing functions.

The availability for organizations to transition to IPv6 is commonly available from ISPs and routing vendors used by network operators. However, IPv4 still produces the majority of network traffic, leaving IPv6 traffic as a minor part of network administration responsibilities in many instances. Having a dual stack IPv4 – IPv6 network requires administrators to have access to the tools, training, and techniques to easily protect assets and understand the different attack vectors that can be used for each protocol.

While not directly related to DNS, IPv4 – IPv6 dual stack environments introduce complexities that can lead to vulnerabilities. As illustrated in Figure 10, SMEs developed an attack tree that evaluated and compared a variety of threats, vulnerabilities, and consequences associated with an incomplete IPv6 transition. The provision of domain name resolution services was the critical function impacted by this attack tree and the primary undesired consequence was a loss or DoS affecting the critical function. SMEs evaluated vulnerabilities associated with the incomplete IPv6 transition, network infrastructure, and Internet routing. These vulnerabilities could be exploited by both deliberate and unintentional threat actors. In the case of a deliberate threat, IPv6 neighbor discovery is a possible threat vector. Possible threat vectors in the case of an unintentional threat include implementation errors and network address translation.

[13] Jackson, William. "Easy-to-use attack exploits IPv6 traffic on IPv4 networks." *GCN.* 4 April 2017. http://gcn.com/Articles/2013/08/09/IPv6-attack.aspx?Page=1.

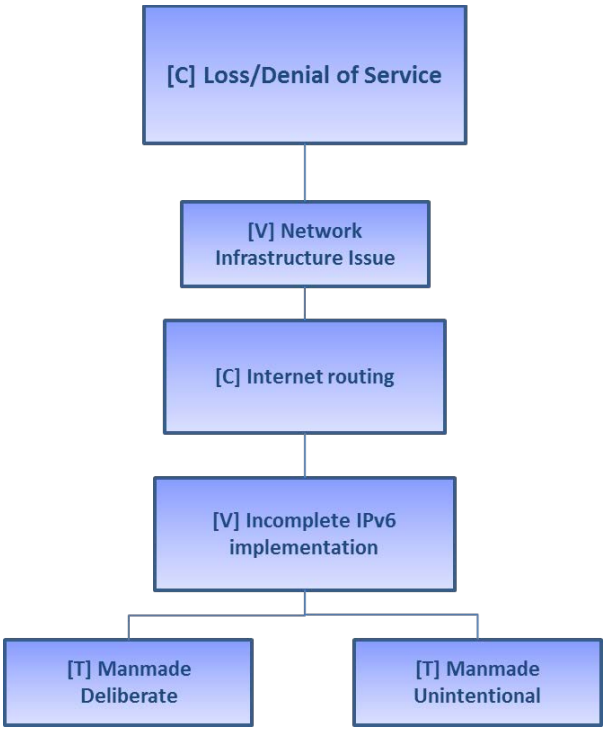

Figure 10: Incomplete IPv6 Transition Attack Tree Summary

The transition from IPv4 to IPv6 will solve the problem of a shortage of IPv4 addresses. While the transition is underway, IPv4 will remain an active protocol in the future. There are a number of options available to facilitate the transition including parallel IPv4 and IPv6 networks, dual stacking, tunneling, and Network Address Translation (NAT). With many internal networks retaining IPv4 addresses, dual stack environments (where IPv4 and IPv6 content are simultaneously hosted) remain common during the transition period. Users without the capability to create a dual stack environment can tunnel IPv6 packets onto IPv4 packets, enabling them to use the existing IPv4 infrastructure. Users can also use NAT to translate IPv6 packets into IPv4 packets.

5.2. Incomplete IPv6 Transition: Risk Assessment

Possible consequences associated with an incomplete IPv6 transition include traffic redirection, DoS, and data loss. Security vulnerabilities can emerge when using transition-enabling methods. SMEs determined that the IPv6 transition vulnerabilities related to employees included the lack of adherence to security best practices and inadequate investment in safeguards. It was also noted that vulnerabilities in processes included the lack of network traffic filtering, quality control, and auditing. In a dual stack environment, firewalls can be misconfigured to apply filtering only on IPv4 traffic and miss IPv6 traffic altogether. Similarly, an IPv4 network broadcasting DNS resource records specific to IPv6 (“AAAA” records) can be targeted with IPv6 packets that may not be monitored.

SMEs determined that the openness of DNS technology was a potential vulnerability because open recursive servers and authoritative servers process packets without verifying their origin. Such a default configuration combined with an incomplete IPv4 to IPv6 transition leaves much

of the DNS infrastructure open to DoS attacks. Both recursive resolvers and authoritative servers will continue to process packets unless their configurations are changed either to filter or to monitor IPv4 and IPv6 traffic to prevent a DoS or damage to the DNS infrastructure itself. Figures 11 and 12 depict these vulnerabilities. In addition, networks broadcast DNS resource records that could allow bad actors to learn about certain aspects of a network's configuration.

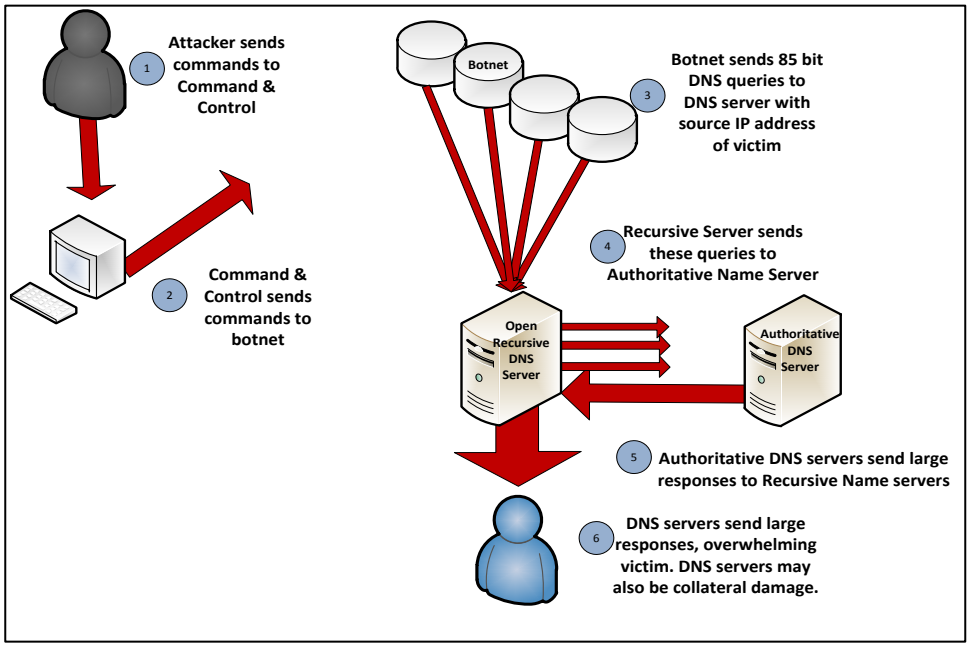

Figure 11: Open Recursive Server DoS Attack

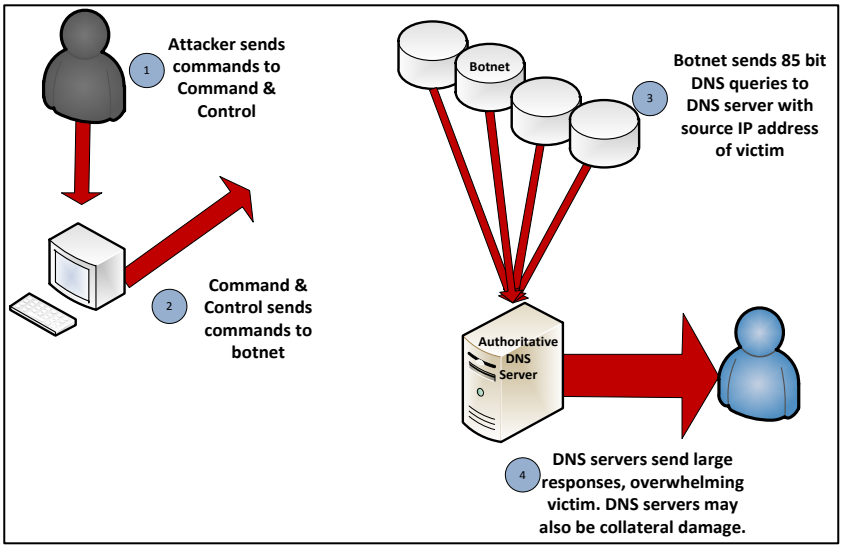

Figure 12: Authoritative Server DoS Attack

SMEs identified nation states, organized crime, and hacktivists as potential deliberate threat actors. Additionally, untrained or careless employees and third-party contractors were identified as potential unintentional threat actors. SMEs expect to have extensive financial resources with a lower level of financing available to other deliberate threat actors. A deliberate threat actor would need a high degree of technical capabilities to be successful since tools to exploit the transition to IPv6 are not readily available. The largest threat from unintentional threat actors are untrained employees that have logical access to relevant systems. The motives for a deliberate attack ranged from DoS to theft, which would affect the availability of accessible data.

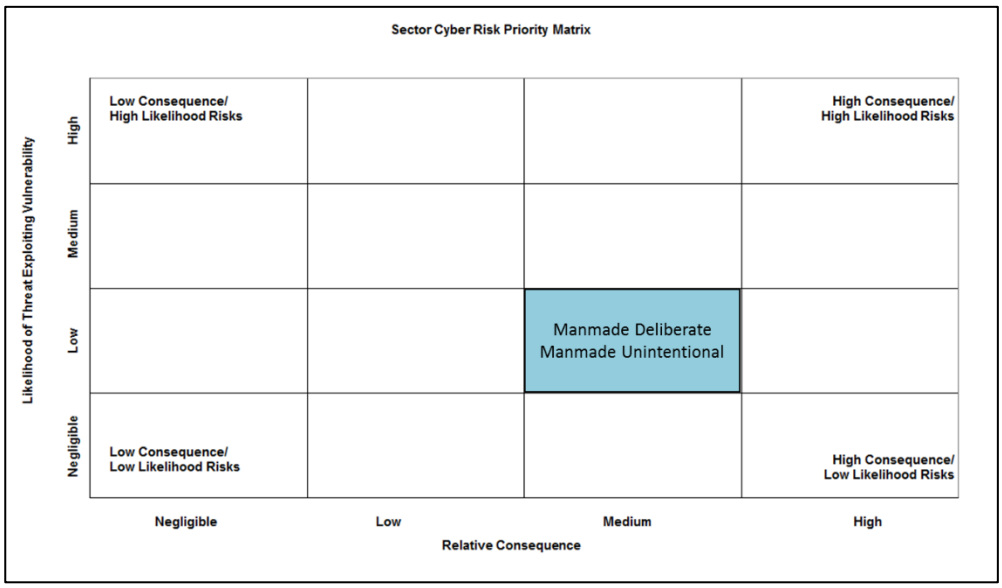

Figure 13: Incomplete IPv6 Transition Risk

5.3. Incomplete IPv6 Transition: Mitigations and Recommendations

People, process, and technology vulnerabilities associated with the transition to IPv6 are currently mitigated with a variety of responses. These vulnerabilities are present in varying degrees among many of the transition methods such as creating dual stack environments or using NAT.

To mitigate vulnerabilities introduced by the people involved with IPv6 transition, owners and operators use:

- Education and training;
- Supervision; and
- Security compliance audits.

To mitigate vulnerabilities introduced by the processes involved with IPv6 transition, owners and operators use:

- Best current practices on IPv6 implementation;

- Change management; and
- Incident response and incident management plans.

To mitigate vulnerabilities introduced by the technologies involved with IPv6 transition, owners and operators use:

- Configuration management;
- Rate limiting;
- DNSSEC;
- Ingress network filtering; and
- Source address verification.

6 Increased Attack Surfaces – Mobility and IoT

6.1. Increased Attack Surfaces – Mobility and IoT: Background

As Internet-connected devices continue to multiply, the number of devices vulnerable to attack and the capacity for hackers to use those devices in and for an attack increases.[14]

The rapid increase of Internet-connected devices follows the maturation of the mobile device industry over the last two decades. The continued growth of the mobile device industry, combined with the explosion in IoT device deployment, will dramatically increase the overall attack surface of organizations. Some estimates assert that that the number of connected devices could surge from 15 billion in 2015, to 200 billion by 2020,[15] and every new device adds a potential attack vector into an organization.

IoT-based attacks are on the rise, putting data, revenue, and reputation at risk. If a DNS service provider goes down, organizational Internet connectivity fails and some devices that are attached to the network lose connectivity. Even a single serious attack can expose data or bring business operations to a halt. While society becomes more connected and technology more ubiquitous, securing systems, networks, and data becomes increasingly important for individual safety, economic security, and national defense.[16] Because there is a high market demand for IoT technology, some IoT devices are hastily deployed and security is not a major consideration. Because of IoT insecurity, many organizations' services were disrupted after their DNS provider experienced a severe DDoS attack with IoT devices being the primary attack vector.[17][18]

With the growing number of Internet-connected devices, the infrastructure and protocols that current DNS and routing operations use may not be sufficient to support the future vision or growth of these devices. This growth could lead to a service breakdown if current security practices are not upgraded, causing both a knowledge failure affecting the *Provide Domain Name Resolution Services* critical function as well as potentially large-scale DoS effects on the *Provide Internet Routing, Access and Connections Services* critical function. SMEs identified two potential vulnerabilities associated with the risk topic: 1) the inability to scale infrastructure, and 2) the lack of a modeling capability to project the exponential strain on routing network resources. In addition, current infrastructure has experienced rapid growth and

---

[14] Hill, Kashmire. "The Half-Baked Security of Our 'Internet of Things'." 27 May 2014. <http://www.forbes.com/sites/kashmirhill/2014/05/27/article-may-scare-you-away-from-internet-of-things/>.
[15] Sun, Leo. "What to Watch in 2017."*The Motley Fool*. The Motley Fool, 23 Nov. 2016. Web. 10 May 2017. <https://www.fool.com/investing/2016/11/23/iot-stocks-what-to-watch-in-2017.aspx>.
[16] Neustar. "Worldwide DDoS Attacks & Protection Report." (n.d.): n. pag. Oct. 2016. Web. 1 Apr. 2017. <https://ns-cdn.neustar.biz/creative_services/biz/neustar/www/resources/whitepapers/it-security/ddos/2016-fall-ddos-report.pdf>.
[17] Paganini, Pierluigi. "OVH Hosting Hit by 1Tbps DDoS Attack."*Security Affairs*. Security Affairs, 25 Sept. 2016. Web. 10 May 2017.
[18] Hilston, Scott. "Dyn Analysis Summary of Friday October 21 Attack." *Dyn Blog*. Dyn, 26 Oct. 2016. Web. 10 May 2017. <http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/>.

demand on network resources, and potential vulnerabilities evaluated in this assessment require further research.

As a primary technology enabling the Internet, DNS is also one of the most important components in networking infrastructure. In addition to delivering content and applications, DNS also manages a distributed and redundant architecture to ensure high availability and quality user response time—so it is critical to have an available, intelligent, secure, and scalable DNS infrastructure. If DNS service is disrupted, most web applications will fail to function properly.[19]

DNS is the backbone of the Internet, but it is also one of the most vulnerable points in the network. Due to the crucial role it plays, DNS is a high-value security target. DNS DDoS attacks can flood DNS servers to the point of failure or hijack the request and redirect requests to a malicious server. To prevent this, a distributed high-performing, secure DNS architecture, and DNS offload capabilities should be integrated into the network.

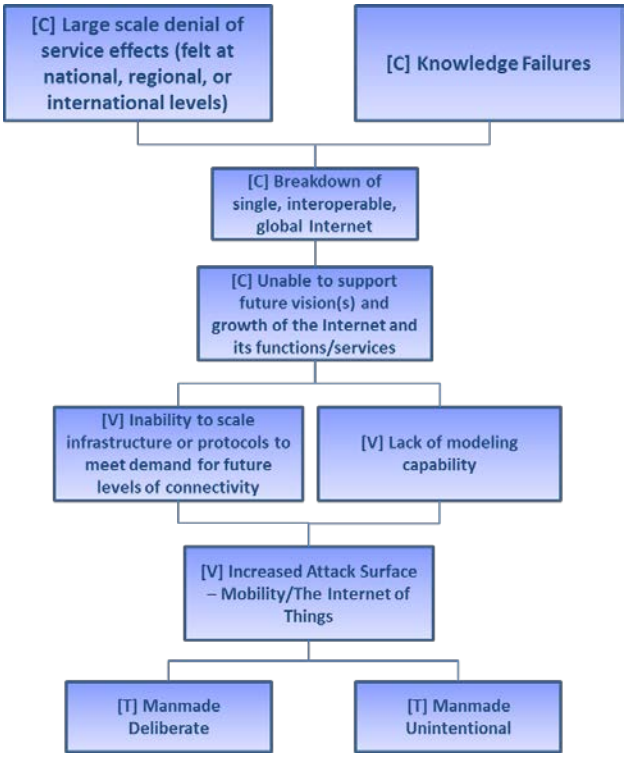

Figure 14: Increased Attack Surfaces Attack Tree Summary

Recognizing that mobile computing will continue to remain the preferred platform for end-user interaction, threats will continue to target users and communities by developing new attack

[19] Velazquez, Marron. "The F5 Intelligent DNS Scale Reference Architecture. *"The F5 Intelligent DNS Scale Reference Architecture*. F5 Networks Inc., 28 Nov. 2013. Web. 01 Apr. 2017. <https://f5.com/resources/white-papers/the-f5-intelligent-dns-scale-reference-architecture>.

techniques and redeveloping existing attack methods. Vulnerabilities exist as architectures and platforms rapidly change to accommodate these fast growing environments and attackers attempt to take advantage of technologies and processes where mitigating activities have not been developed or managed properly. Any device with low levels of security added to the network can potentially provide an attacker with new attack surfaces.

As DNS and Internet routing infrastructure continue to increase in scale to meet the demand for future levels of connectivity, there are several challenges. For mobile devices in particular, cross-sector and boundary provisioning may cause problems as multiple providers are involved in the provisioning process for a single device. This also requires a variety of authorizations as the traffic moves, potentially making it possible to see routing information. For the IoT, networked items have relatively little memory and are limited in their computational capacity, which makes them susceptible to threats like DoS attacks, route injection, and hijacking.

6.2. Increased Attack Surfaces – Mobility and IoT: Risk Assessment

The impacts of an increased attack surface are felt not just by DNS providers, but by those who manage and defend enterprise networks. Organizations face an uphill battle, as the attack surface needing protection has grown significantly and is expected to balloon even further. In the past, organizations focused on network and endpoint protection, but currently, applications, cloud services, mobile devices (e.g., tablets, mobile phones, Bluetooth devices, and smart watches), and IoT represent a broadly extended attack surface. According to the 2015 Global Risk Management Survey, 84% of cyber-attacks target the application layer and not network layer, requiring a more holistic approach to cyber security.[20]

Undesired consequences, such as DoS and traffic redirection, will result from attackers taking advantage of IoT vulnerabilities. Large amounts of hijacked routes can affect the proper operation of routing tables for DNS operators. Operators, organizations carrying the devices, and end-users may see significant consequences, including the loss of data and financial assets or possible physical damage to networked devices. By controlling a significant number of devices, attackers would be able to create a ‘zombification’ or compromise effect for entire environments. This would allow the zombie devices to be used in large-scale DoS attacks or to spread malware, affecting the ability of DNS operators to control communications. [21] The Mirai botnet used to take down the DNS provider of many large content providers was comprised of several IoT devices by turning the devices into zombie nodes. The Mirai botnet attack registered as one of the largest DoS attacks recorded. Not only do these devices have the power to disrupt by exploiting vulnerabilities en masse, but each device can potentially introduce a potential vector an attacker could use to gain access to network data or infrastructure.

---

[20] Risk Sense White Paper | The New Enterprise Security Model: Cyber Risk Management. "The New Enterprise Security Model." (2016): n. pag. July 2016. Web. 1 Apr. 2017. < https://risksense.com/_api/filesystem/312/RiskSense-WP_The-New-Enterprise-Security-Model_07292016.pdf >.

[21] These infected devices are referred to as “zombies” because the owner tends to be unaware of the infection

Vulnerabilities introduced by the personnel, processes, technologies, and physical infrastructure associated with the IoT can be exploited to create instability in growth of the Internet and the DNS and Internet routing functions. End users play an important role in their computing environments and the lack of adherence to recognized policies and standards make those environments more susceptible to attack. As part of their risk management strategy, DNS operators continue to invest in high-quality safeguards for growing infrastructure. These security capabilities play an important role in minimizing the risk. The introduction of IoT devices into society has created an influx of device vendors building hardware and software that potentially introduce new vulnerabilities into a network. While the IoT industry continues maturing, the various technologies used to build their devices.

The increase in the complexity of management processes could lead to inadequate quality control and auditing, as well as a lack of resource management across platforms. Unique to the scale of mobile computing and IoT, network traffic filtering and the size and scale of routing tables may become too complex to operate under current processes.

Because much of the control moves from the administrator to the end-user in these environments, device configuration will also depend on the user. The inherent default openness of the technologies and lack of security features also make the devices more exploitable. For DNS operators, infrastructure technology may not be adequate to handle certain protocols once the number of connected devices reaches a certain scale. This infrastructure can include protocols and platforms, routing hardware, fiber, memory, and the physical configuration of IP addressable objects.

Threat actors are continuously looking to exploit the expanding attack surface created by the IoT. Nation States or sponsored actors of nation states are good examples of most common deliberate actors. Organized criminals and hacktivists may also have the capabilities required for exploiting IoT vulnerabilities. These actors may seek to cause large-scale DDoS attacks on DNS infrastructure. They may also have the ability to redirect Internet traffic, resulting in the theft or damage of data. Nation states can also redirect traffic to censor the tools end-users use to communicate, gain access to end-user personal information, or cause damage to other nation states' political reputation

Due to the complexity of most organizations enterprise environmental handling of the IoT, threat actors require a sophisticated level of technical expertise, route hijacking, script, or other tools, and in certain situations access to wireless networks to produce an attack within their targeted environment. In the case of large-scale targeting or logical access to a single device in an interconnected mobile environment, threat actors would also require logical access to DNS operator networks. This access can now come from a wide variety of IoT devices that are capable of "phoning home" to a command and control node belonging to an unauthorized actor.

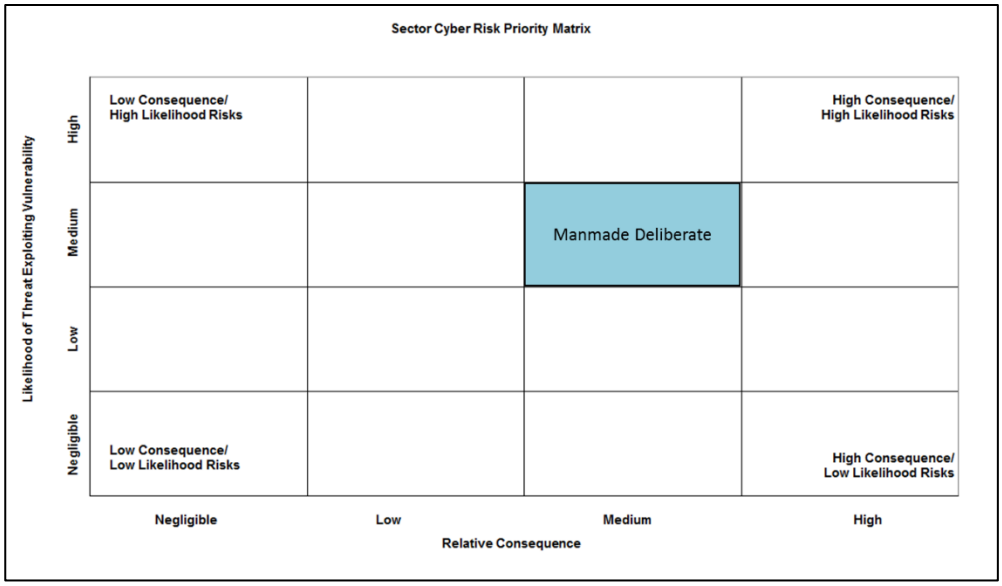

Figure 15: Increased Attack Surfaces Risks to the Provide Domain Name Resolution Services and Provide Internet Routing, Access and Connection Services Functions

6.3. Increased Attack Surfaces – Mobility and IoT: Mitigations and Recommendations

SMEs evaluated existing mitigations, but recognized that these responses may not mitigate future vulnerabilities as the number of attack surfaces rapidly grows. As DNS operators receive an increasing number of responsibilities, and as the amount of people, processes, technologies, and physical infrastructure involved with programming and device management grows, vulnerabilities associated with these factors will also increase. In sum, current mitigations are appropriate to manage most current threats, but additional mitigation features most likely will need to be developed to meet future threats.

To mitigate vulnerabilities introduced by the people involved with mobile device use and the IoT, owners and operators use:

- Recognized policies and standards;
- Employee supervision; and
- Security compliance auditing.

To mitigate vulnerabilities introduced by the processes involved with mobile device use and the IoT, owners and operators use:

- Ingress and egress network filtering, particularly looking for open IoT devices or Command and Control nodes;
- Resource management practices;
- BGP best deployment practices; and
- Encryption protocols used regularly.

To mitigate vulnerabilities introduced by the technologies involved with mobile device use and the IoT, owners and operators use:

- IP source validation; and
- IP route leak and hijacking detection.

To mitigate vulnerabilities introduced by the physical infrastructure involved with mobile device use and the IoT, owners and operators use:

- Hardware capacity modeling and simulation;
- Training to educate users about the potential impact of using insecure IoT devices; and
- IP configuration best practices to ensure new infrastructure can support the user base.

Network operators, standards development organizations, and government agencies can promote and support DNS and Internet routing functions through several actions, including:

- Education to increase security hygiene and awareness of end-users ultimately responsible for the security of devices and the environments they are deployed in; and
- Device interfaces to increase the ability for end users to ensure correct security protocols are being used.

7 Lack of SAV

7.1. Lack of SAV: Background

Because of the difficulty involved, DNS resolvers, both open recursive and authoritative, cannot screen incoming network traffic to ensure that it originates from its stated source. In March 2013, a non-profit organization's website was the target of a DDoS attack that exploited the open nature of the organization's open recursive servers. The organization could have defended against such a DDoS attack by implementing SAV and filter packets from a predetermined range of IP addresses.[22]

SAV is a set of methods to verify that the source IP addresses submitted to a DNS server are valid. SAV ensures that the packets are not assigned from private addresses and are from an acceptable range of IP addresses. As a result, packets from unknown, untrusted, or spoofed sources cannot be processed by the DNS infrastructure. Because recursive DNS resolvers and authoritative DNS servers are usually set to respond to packets either automatically or without verifying the sender's source address, a lack of SAV could lead to DNS resolvers and authoritative DNS servers being overwhelmed with packets or enabling a DoS attack through response amplification.

SMEs evaluating the importance of SAV stressed the importance of incorporating this technique in network operations as one of the only reliable ways to prevent spoofing of IP addresses. Communications SMEs evaluated an attack tree, illustrated in Figure 16, which explored the lack of SAV and a variety of associated threats, vulnerabilities, and consequences. The provision of domain name resolution services was the critical function impacted by this attack tree and the primary undesired consequence was a loss or DoS impacting the critical function. A secondary undesired consequence was a large-scale attack on DNS infrastructure. SMEs evaluated a lack of SAV, and additional vulnerabilities including the configuration of open recursive DNS resolvers and unrestricted traffic responses from authoritative DNS resolvers as the primary vulnerabilities. The SMEs determined that the lack of SAV could be exploited by deliberate effort, which led to the evaluation of deliberate threats only.

[22] Mohan, Ram. "Good neighbors know: Now is the time for source address validation." *Security Week.* 7 May 2013. http://www.securityweek.com/good-neighbors-know-now-time-source-address-validation.

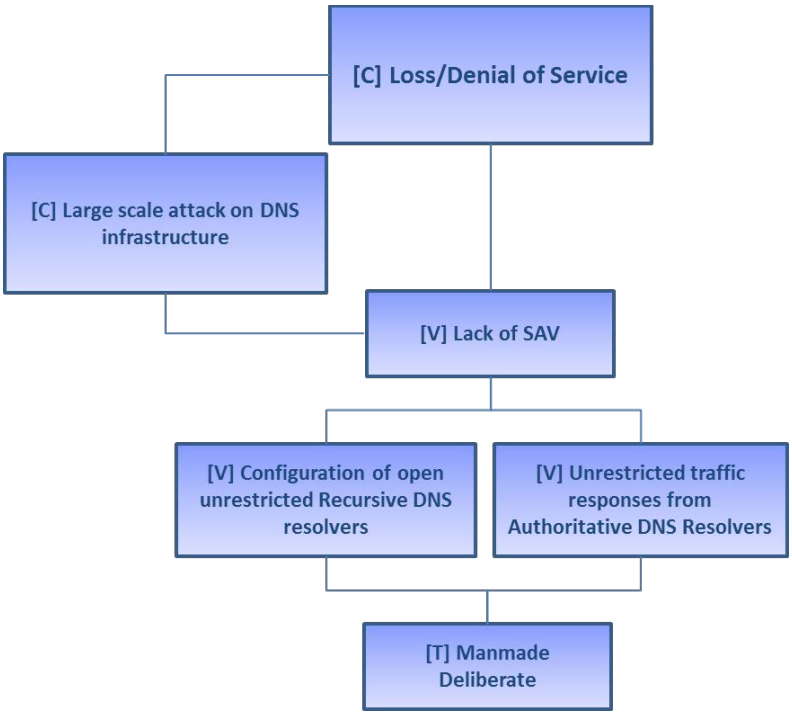

Figure 16: Lack of SAV Attack Tree Summary

7.2. Lack of SAV: Risk Assessment

SMEs identified traffic redirection, DoS, data loss, and identity theft as possible consequences of a malicious actor exploiting vulnerabilities associated with the lack of SAV. Among open recursive DNS resolvers and authoritative DNS servers, SMEs identified several vulnerabilities, including the inadequate investment in safeguards, lack of network traffic filtering, inadequate quality control, and the inherent openness of the DNS infrastructure. At the same time, SMEs said that some measures were already in place to mitigate against threats to the open DNS infrastructure.[23] SMEs noted that some recursive DNS resolvers and authoritative DNS servers had ingress network filtering, limits on recursion on name servers, IP address validation, response rate limiting, and DNSSEC as security measures against potential attacks. They outlined several process-oriented measures to protect lack of SAV vulnerabilities, including security policy compliance audits, education, and awareness.

Potential actors ranged from nation states and organizations sponsored by nation states, to organized crime and hacktivists. Nation states were likely to have a high degree of financial resources while organized crime and hacktivists were likely to have fewer financial resources. Regardless of the threat actor, existing tools to spoof or hide IP addresses could be used to take advantage of the lack of SAV and launch DoS attacks. The motives for such an attack could

[23] Network operators, standards development organizations, and government agencies can play roles in promoting and supporting SAV implementation by deploying methodologies described in BCP 38 (http://tools.ietf.org/html/bcp38)

range from censorship by a nation state against specific targets to corporate espionage for organized crime and the publicity of an attack for hacktivists.

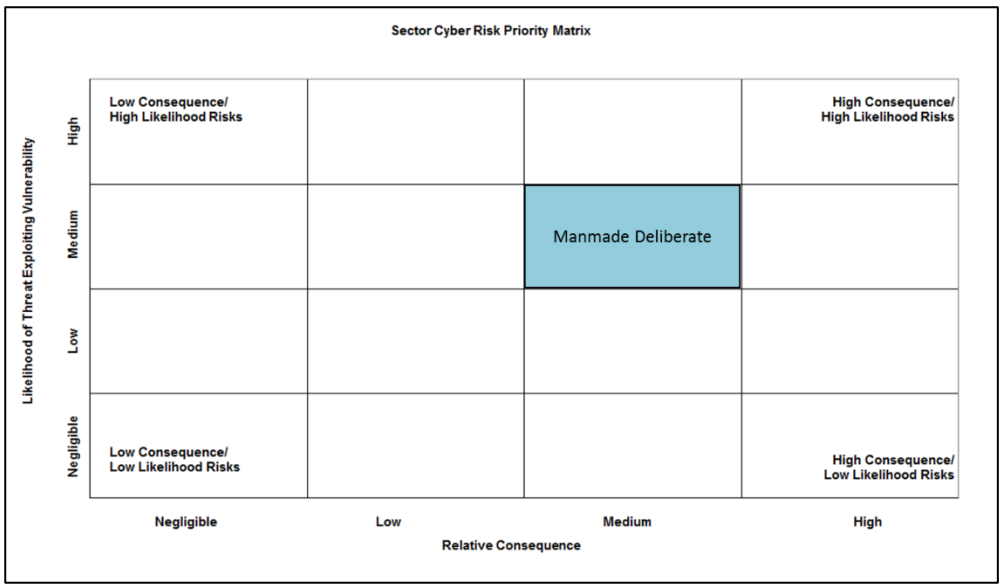

Figure 17: Lack of SAV Risks to the *Provide Internet Routing, Access and Support Services* Function

7.3. Lack of SAV: Mitigations and Recommendations

People, process, and technology vulnerabilities associated with a lack of SAV are currently mitigated with a variety of responses.

To mitigate vulnerabilities introduced by the people involved with SAV, owners and operators use:

- Best current practices on IP source validation;
- Supervision; and
- Education and awareness.

To mitigate vulnerabilities introduced by the processes involved with SAV, owners and operators use:

- Security policy compliance and audits;
- Closing down an operator (i.e. domain name registrars, ISPs, hosting providers) when necessary; and
- Incident management and incident response plans.

To mitigate vulnerabilities introduced by the technologies involved with the SAV, owners and operators use:

- Limits on recursion on name servers;
- Response rate limiting;

- Ingress network filtering; and
- DNSSEC.

8 Route Injection/Hijacking

8.1. Route Injection/Hijacking: Background

Malicious actors can compromise servers that hold DNS records for a given domain name. By changing the DNS records, malicious actors can redirect traffic to a Website that they control.[24]

A route injection or hijacking occurs when a threat actor gains access to routers running BGP and alters or injects their own route. Physical access is not necessary to exploit a vulnerability if the router can be found on the Internet. While an insider would have quicker access to the network, logical access is all that is required to perform an attack. A third-party vendor or an untrained network operator can inadvertently cause the same types of issues. Entities are currently relying on filters to discover the alternate routes. However, a savvy attacker will attempt to choose an injection point that can target a block of IP addresses while avoiding the filters in place.

SMEs identified three tiers of consequences, with the top tier undesired consequence being a partial or complete loss of the Internet routing critical function. A disruption or an information confidentiality breach is a top tier undesired consequence that would impact inter-domain connectivity and result in the loss of the Internet routing critical function. In order to achieve these consequences, attackers could exploit improper BGP configuration. Malicious actors could inject a multi-hop route and introduce an outside router. These actions could result in a man-in-the-middle attack, the acquisition of routing information through sniffing, the introduction of fake routing information, false BGP updates, or prefix hijacking. Unintentional threats come from the owners, operators, or vendors who fail to thoroughly test BGP configuration changes or implement configurations improperly. As illustrated in Figure 18, SMEs identified several vulnerabilities and threats that could lead to undesired consequences within the topic.

[24] Cubrilovic, Nik. “The Anatomy of The Twitter Attack: Part II.” Techcrunch. 18 December 2009. http://techcrunch.com/2009/12/18/anatomy-twitter-attack-2-dns-iran/.

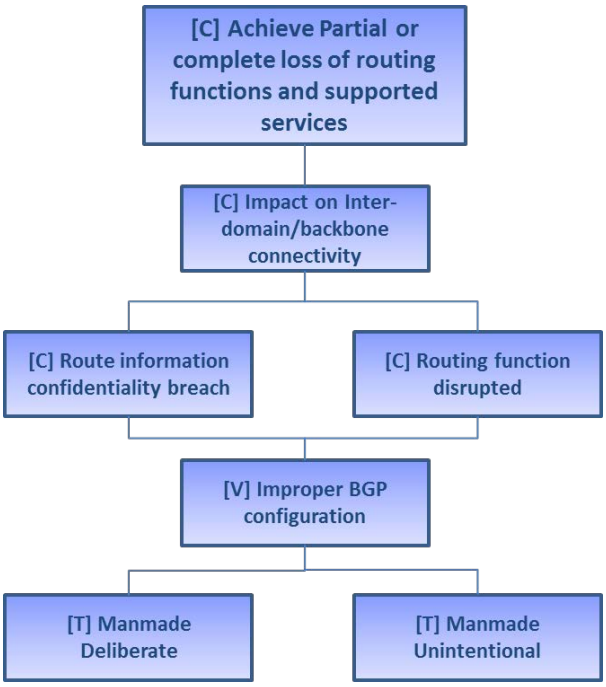

Figure 18: Route Injection/Hijacking Attack Tree Summary

8.2. Route Injection/Hijacking: Risk Assessment

The redirection of traffic could lead to a DoS, a loss of data and financial assets, and the loss of reputation or image for an entity in the long-term. DNS and Internet routing functions would be directly affected and the remaining functions would be indirectly affected by such a redirection. However, upon detection the issue can be resolved within hours bringing the fully recovered system back to order.

Personnel vulnerabilities were seen as the most important because of access issues. SMEs identified insufficient background checks and social engineering as potential points of weakness. Another problem is privilege creep, when employees retain their privileges even after those privileges no longer pertain to their positions or job requirements. SMEs identified change management within the technology structure as well as the need for patch management and updates to systems as the main technology vulnerabilities. A lack of redundancy in the system location could also lead to an exploitable vulnerability.

SMEs determined that a nation state, criminal, or hacktivist would be the most likely deliberate threat actors. Their primary objective likely would be a demonstration of their power, or ability to disrupt routes within the organization. While the disruption of business or government work is a by-product of this objective, SMEs concluded that this likely would not be sole objective. The attack's intended outcome would likely be to damage, or impair the usefulness of the system in their attempts to shut it down entirely. The actor could potentially acquire business processes or assets if the actor is a part of a well-funded nation state.

As physical access is not required, there is a higher chance the actor can act in the same capacity as an authorized insider. However, logical access is required. Therefore, the threat actor would

need to be able to gain access via a proxy if necessary. Once in the system, the actor would seek to exploit the gained entry to redirect or inject alternate routes. If the actor is working with a nation state or other highly organized group, they would wish to remain hidden while they achieved their goal. A hacktivist group would want their exploitation of the entity's system to be widely known. This actor would have minimal constraints with one exception – they would attempt to achieve the disruption without completely disabling Internet routing so that they would not affect their own desired outcome.

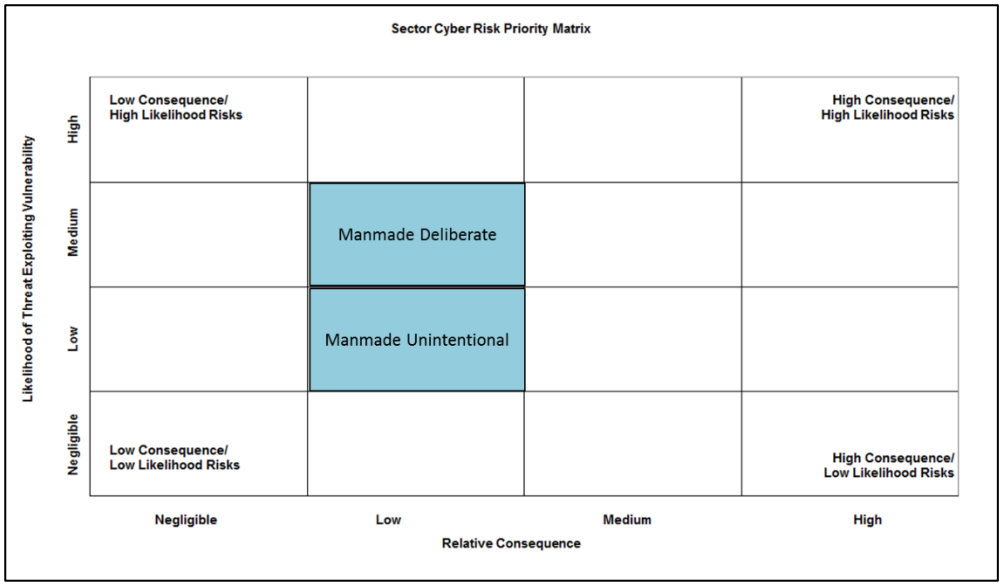

Figure 19: Route Injection/Hijacking Risks to the *Provide Internet Routing, Access and Support Services* Function

8.3. Route Injection/Hijacking: Mitigations and Recommendations

People, process, and technology vulnerabilities associated with route injection/hijacking are currently mitigated with a variety of responses. To mitigate vulnerabilities introduced by people that could lead to route injection or hijacking, owners and operators use:

- Monitoring of administrative privileges and access levels adhere to strict staff vetting procedures, performing background checks, and applying standards in the vetting process.

To mitigate vulnerabilities introduced by processes that could lead to route injection or hijacking, owners and operators use:

- Best practices following recognized policies and standards; and
- Procedures evaluations (internal teams, Inspector General) to ensure compliance.

To mitigate vulnerabilities introduced by technologies that could lead to route injection or hijacking, owners and operators use:

- Separation of BGP privilege levels and leverage external BGP route monitoring tools;
- Maintenance and testing of the ability to de-aggregate routes; and

- Maintenance of:
    - Asset Management accreditation and certifications; and
    - Resource Public Key Infrastructure Equipment & Route Certifications.

9 SSL Implementation Errors

9.1. SSL Implementation Errors: Background

Flaws in implementing SSL communications could lead to browsers accepting spoofed certificates as authentic. A hacker could obtain a legitimate certificate issued to a hacker-controlled domain and then take advantage of implementation flaws in SSL communications to appear legitimate.[25]

SMEs identified two overarching undesired consequences: (1) policy, governance and knowledge failures; and (2) loss or DoS. Under a loss or DoS, SMEs identified a DNS system issue or a large scale attack on DNS infrastructure as another tier of consequences. SMEs determined that vulnerabilities that could lead to these undesired consequences include a system failure (either hardware or software); unknown levels of redundancy and resiliency; a lack of quality assurance testing, code, and operational deployment review; a lack of modeling and simulation; and unsecure or incorrect coding. Threat actors could exploit these vulnerabilities deliberately or unintentionally. Figure 20 describes the vulnerabilities and threats that SMEs identified that could lead to undesired consequences within this topic.

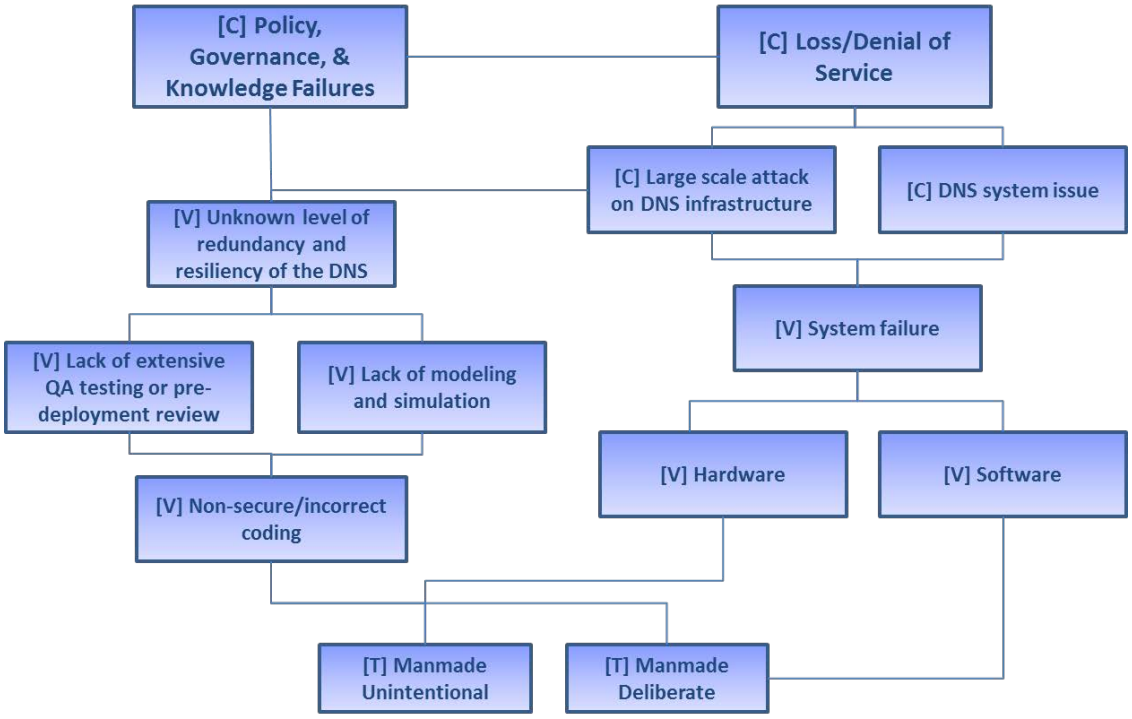

Figure 20: SSL Implementation Errors Attack Tree Summary

Inappropriate or incorrect implementation of hardware or software can lead to a variety of issues within a system. Within the DNS realm, implementation flaws may cause security

[25] "Vulnerabilities Allow Attacker to Impersonate Any Website." Wired. 29 July 2009. http://www.wired.com/2009/07/kaminsky/.

vulnerabilities that can be exploited by DoS attacks, data theft, cache poisoning, and network penetration. While the Heartbleed incident did not relate to DNS specifically, it is an example of how damaging even a minor flaw can be to the Internet infrastructure.[26] In the case of DNS, there are several areas where incorrect implementation can occur. While network administrators may have knowledge of their own systems and DNS in general, network administrators may have limited knowledge about the upgrades they are making (e.g., DNSSEC, upgrading to IPv6). This can open the door to a wide range of possible implementation flaws that can leave networks vulnerable to attack.

9.2. SSL Implementation Errors: Risk Assessment

SSL implementation errors associated with new software and hardware installation could cause significant problems with DNS resolution. These problems could then lead to DoS, traffic redirection, data theft, and network penetration. Implementation flaws in open recursive DNS servers could be exploited by server attacks like DNS cache poisoning to redirect users to malicious websites or to be used to carry out DoS attacks.

Vulnerabilities associated with implementation errors are varied. Employees could suffer from a lack of technical and operation management expertise as well as non-adherence to best practices. Similarly, inadequate auditing could result in processes that fail to detect implementation flaws. Physical problems with the hardware itself or faulty installation could cause connectivity issues and performance degradation. There could also be a lack of interoperability between existing and newly installed hardware and software. SMEs noted that there are several risk mitigations already in place, including existing interoperability testing, monitoring, audits, and quality assurance.

SMEs identified nation states, organized crime, hacktivists, and disgruntled customers or vendors as potential threat actors. These actors likely would seek to deny service, penetrate networks, and redirect traffic. Threat actors would need to know about an implementation flaw in order to exploit one, but malware and scripts to exploit these flaws are well-known and available. SMEs also noted that threat actors exploiting implementation flaws were likely to be adept with the tools and technology needed to carry out an attack while financial resources would be dependent on the type of threat actor. Logical access to the implementation flaw is needed, and the type of access that a threat actor would have depends on the actor's resources. For example, an organization sponsored by a nation state or a criminal syndicate is likely to have insider access while hacktivists are likely to gain access through a third-party vendor or outside contractor with the appropriate privileges.

[26] The Heartbleed bug is a vulnerability found in the OpenSSL cryptographic software library. The vulnerability compromises the security keys used to identify service providers and encrypt user traffic, usernames, passwords, and content. This underlying implementation flaw would allow individuals to steal protected information used to secure Internet communication security and privacy. http://heartbleed.com/

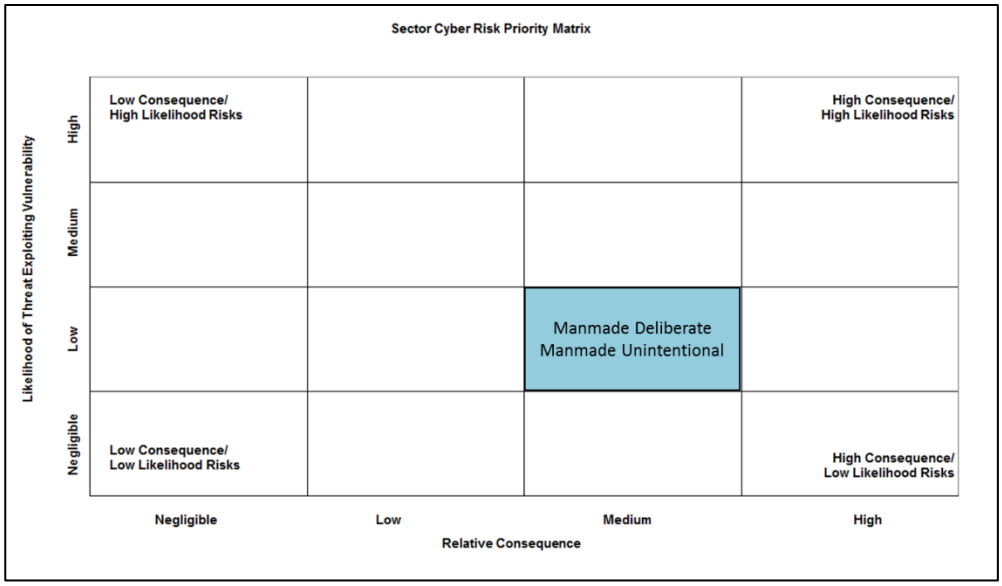

Figure 21: SSL Implementation Errors Risks to the *Provide Domain Name Resolution Services* Function

9.3. SSL Implementation Errors: Mitigations and Recommendations

People, process, and technology vulnerabilities associated with implementation flaws are currently mitigated with a variety of responses.

To mitigate vulnerabilities introduced by the people involved with implementing SSL communications, owners and operators use:

- Education and training;
- Recognized policies and standards; and
- Employee monitoring, auditing, and oversight.

To mitigate vulnerabilities introduced by the processes involved with implementing SSL communications, owners and operators use:

- Auditing;
- Change management practices;
- Configuration management practices;
- Interoperability testing;
- Monitoring of advisories; and
- Incident response practices.

To mitigate vulnerabilities introduced by the technologies involved with implementing SSL communications, owners and operators use:

- Intrusion detection systems;
- Implementation of best practices on secure coding; and
- Quality assurance and modeling and simulation techniques.

10 Stewardship of the Internet's Technical Identifier Resources

11.1. Stewardship of the Internet's Technical Identifier Resources: Background

The planning and management of a set of interdependent technical functions have the potential to affect user Internet traffic. Specifically, these functions include the processing of changes to the authoritative root zone file of the DNS and DNSSEC root key signing key management, the allocation of Internet numbering resources, and the coordination of the assignment of technical Internet protocol parameters.

Planning and management of these interdependent DNS technical functions have the potential to affect user Internet traffic. These technical functions include:

- Process changes to the authoritative root zone file of the DNS and root key signing key management;
- Allocation of Internet numbering resources; and
- Coordination of the assignment of technical IP parameters.

Stewardship of these technical functions is critical to the effective engineering and operational controls that currently support a single, global, interoperable Internet. Stewardship entities need the technical competence to manage these functions and changes in stewardship might have negative effects on proper management. SMEs noted the importance that process controls play on implementing root zone changes and the need for security and redundancy of root zone physical facilities.

11.2. Stewardship of the Internet's Technical Identifier Resources: Risk Assessment

In the process of conducting the risk assessment, SMEs recognized that ongoing activities in the DNS and Internet stewardship environments may have implications on the IT Sector's risk profile. To fully assess potential risks to the topic, SMEs expressed the desire to evaluate the topic in future work.

11.3. Stewardship of the Internet's Technical Identifier Resources: Mitigations and Recommendations

SMEs recognized the importance of stewardship of these technical functions associated with technical identifier resources on the IT Sector's provision of DNS. The SMEs expressed interest in fully evaluating the topic in the future once the policy and technical landscape is more clearly defined. The SMEs plan to identify relevant aspects of the topic and provide recommendations at that time.

11 Supply Chain Risk to DNS

11.1. Supply Chain Risk to DNS: Background

DNS and Internet routing infrastructure operators are dependent on the hardware and software used in day-to-day operations and the suppliers of those products. Successful attacks against the supply chain can disrupt systems and networks in a manner that can be difficult to diagnose.[27]

Dependencies on a supply chain are part of most organization's operational models, and DNS services are as susceptible to having vulnerabilities introduced along the supply chain as any other business function. Understanding the risks and impacts caused by disrupting DNS and Routing operations through supply chain vulnerabilities is an important consideration for ensuring continuity of Internet communications.

Due to the connected nature between the *Internet Routing, Access and Connection Services* and *Domain Name Resolution Services* critical functions, SMEs evaluated both functions through a single, supply chain-focused attack tree, illustrated in Figure 22. SMEs recognized that among other vulnerabilities, the introduction of faulty, tainted, or counterfeit products, or lack of supplier choice and product availability, could cause cascading failures to sub-elements of the routing network. For the *Provide Domain Name Resolution Service* critical function, this breakdown could lead to knowledge failures, mainly resulting from the lack of extensive vulnerability and quality assurance testing or operational deployment review. It could also impact routing functions by resulting in a DoS attack across large networks or Internet routing sub-functions dependent on products that are unavailable or not operating effectively. SMEs identified a lack of modeling capability or quality assurance as significant vulnerabilities that could be exploited by attackers or unintentional manmade actions.

[27] Leyden, John. “Experts argue over whether shallow DNS gene pool hurts web infrastructure.” 16 August 2012. http://www.theregister.co.uk/2012/08/16/shallow_dns_gene_poll/

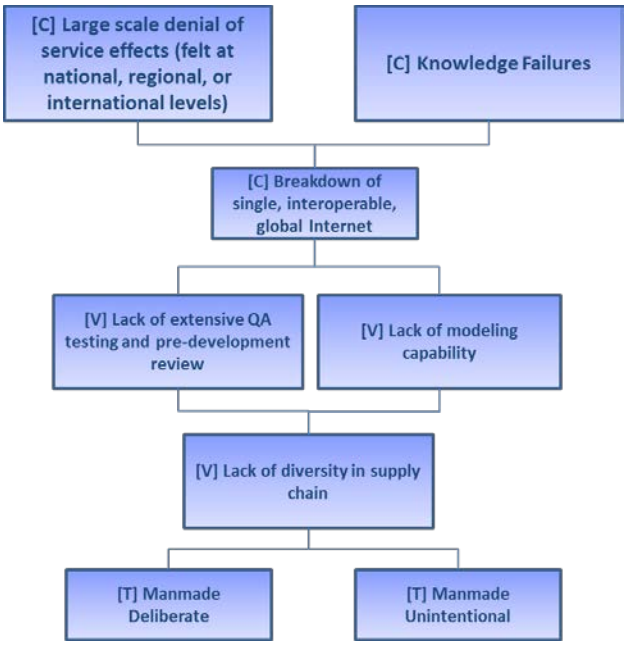

Figure 22: Supply Chain Risk to DNS Attack Tree Summary

As Internet communications rely on DNS, DNS infrastructure relies on the hardware and software that operate and manage its technical capabilities. These hardware and software packages allow for central management of DNS, including data storage, process automation, information security, and deployment. The technical complexity of the software used in DNS provisioning can limit the availability of DNS infrastructure supplies and suppliers. A targeted attack on suppliers can affect the availability and advancement of services and technologies. Exploited vulnerabilities within a single piece of software can have widespread affects across multiple DNS operators. This limited availability may also result in a high concentration of single points of failure within a restricted number of providers.

Similarly, DNS servers often use similar cryptographic modules directly embedded within the operating systems. Depending on operator process protocols, limited sources for these modules can also lead to single points of failure. These failures create cascading affects that result in large-scale DoS effects or knowledge failures disrupting Internet routing and access.

11.2. Supply Chain Risk to DNS: Risk Assessment

Significant consequences can occur due to the lack of diversity in products provided by DNS hardware and software suppliers (e.g., all are dependent on a finite number of shared libraries) and can affect the provision of DNS and Internet routing services. Technical sophistication is also growing and increasingly available to adversaries and attackers. They can use the supply chain to exploit products and processes throughout the development lifecycle and cause disruptions to operations. If counterfeit components are introduced into operations, traffic redirection and denial of service is possible, allowing an attacker to steal data, personal information, and financial assets.

In addition to product concerns, vendors or other third parties in the supply chain may also pose a risk. Personnel, process, technology, and physical infrastructure vulnerabilities are inherent in supply chain operations. Lack of security controls in small organizations with small employee sets, or even a lack of staff resources, can lead to vulnerabilities.

Inadequate peer review processes affect products in the manufacturing process through their implementation into operational networks. Ineffective configuration management or auditing processes can degrade capabilities or render them inoperable. Technical environment complexity often requires that introducing new products into DNS and Internet routing systems require pre-introductory modeling and simulation exercises. Without these processes, operators may not have full awareness of the network response to product introduction.

Physical vulnerabilities mostly reside with the supplier, including manufacturing and delivery. Suppliers with a small number of physical locations can have manufacturing capabilities degraded with the loss of a single facility's operations. Physical delivery and delivery routes can also be attacked or exploited, affecting DNS operations.

The lack of diversity in the DNS and Internet routing hardware and software supply chains may be exploited deliberately and unintentionally. SMEs identified the most common deliberate actor to be nation states or sponsored actors of nation states, while organized criminals and hacktivists may also have the capabilities required for exploitation.

These actors may seek to cause large-scale DoS attacks on DNS infrastructure. They would have the ability to redirect Internet traffic, resulting in the theft or damage of data. By targeting specific suppliers, these actors would also have the ability to affect the advancement of technologies used in DNS infrastructure, resulting in financial gains or corporate espionage.

Threat actors would require a sophisticated level of technical expertise as well as a significant amount of time to identify vulnerabilities that would result in cascading affects along the entire supply chain vertical. Additionally, threat actors would require logical access to DNS operator networks to access control platforms. In some instances, threat actors could look for opportunities for physical access, including employing social engineering techniques against personnel. SMEs noted that physical damage, acts of vandalism, or the destruction of physical supplier facilities might also affect a vendor's ability to provide DNS infrastructure products and services.

In addition, unintentional actors, including third-party contractors and inexperienced or incompetent DNS operator personnel, can also affect DNS provision. Insufficient employee training, improper security, and improper business practices could result in unchecked actions. DNS operators relying on cost-based product source selection may be more prone to vulnerabilities. Because of the evolutionary nature of DNS, single-source technology or testing new technologies developed through singular pioneering production can increase the attack surface.

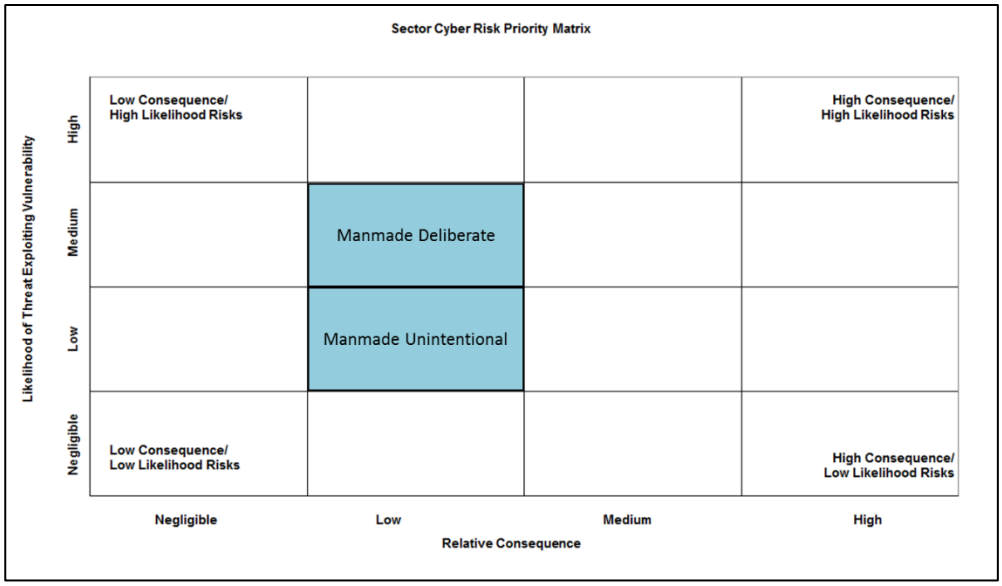

Figure 23: Lack of Diversity in DNS Hardware and Software Suppliers Risks to the *Provide Domain Name Resolution Services* Function

11.3. Supply Chain Risk to DNS: Mitigations and Recommendations

The significant growth in the variety of DNS software solutions over the last several years has led to a greater diversity in vendors, but a component of the DNS landscape still possesses many points of failure. Notably, the use of common shared libraries across multiple implementations, such that while there may be many different pieces of software handling the actual DNS traffic, all of the software leverages common libraries (such as OpenSSL) to do functions such as TLS or some of the crypto libraries used by DNSSEC. These underlying libraries are open to bugs in the same way the resolver code can be, as is demonstrated by the HeartBleed vulnerability of 2015.

People, process, and technological supply chain risks are currently being mitigated with a variety of responses.

To mitigate vulnerabilities introduced by the people involved with hardware and software suppliers, owners and operators use:

- Education and training;
- Recognized policies and standards; and
- Employee monitoring, auditing, and oversight.

To mitigate vulnerabilities introduced by the processes involved with hardware and software suppliers, owners and operators use:

- Change management practices;
- Configuration management practices; and
- Process auditing.

To mitigate vulnerabilities introduced by the technologies involved with hardware and software suppliers, owners and operators use:

- Secure coding best practices;
- Quality assurance;
- Modeling and simulation techniques; and
- Red zone delegation trials to determine how technologies, and the environments they operate in, interact with their entry within an entity's system.

Ultimately, by using a more diverse supplier base when available, operators try to manage against single points of failure.

12 Conclusion

The 2009 ITSRA identified two risks with a moderate or high likelihood of occurrence and three risks that could have a significant impact on the *Provide Domain Name Resolution Services* critical function. In the 2017 update to the *Provide Domain Name Resolution Services* critical function assessment, SMEs determined that there is a moderate likelihood that vulnerabilities in the *Provide Domain Name Resolution Services* critical function will be exploited. However, should a vulnerability be exploited, none of the risk issues are considered by the SMEs who participated in this assessment to have a significant impact on DNS services. This change in potential significance from 2009 to 2017 is due to the globally-distributed nature of the DNS, the redundancies across DNS networks, and the mitigations deployed by DNS operators since 2009.

Regarding the *Provide Internet Routing, Access and Connection Services* critical function risk assessment, the 2009 ITSRA identified one risk that could have a significant impact on the function. However, it was determined that the likelihood of a vulnerability being exploited was minimal. The 2017 assessment determined that risk issue evaluated would no longer have a significant impact on the Provide Internet Routing, Access and Connection Services because of increased diversity in Internet routing infrastructure.

While no significant risks were identified through this assessment, it does not mean that the DNS function is insulated from a successful attack, or that such attacks would not have low-level impacts. The finding is that there is a low likelihood that a cyberattack could cause a significant impact on the DNS function. This assessment could change in the future due to the increasing number of Internet-connected devices, which increases the potential attack surface and increases the burden placed on DNS and Internet routing infrastructure to manage the rising volume of traffic. As such, there is increasing reason for enhancing the security and resilience of DNS and Internet routing. Doing so will require a strong partnership among industry, government, academia, and other stakeholders.

Addressing DNS and Internet Routing risks does not conclude with the release of this report. This assessment identifies areas for future examination. Further, findings from this assessment and other community efforts, can inform enterprise-wide risk management activities by providing an understanding of the risks shared by those in the DNS and Internet routing community. As the risk landscape changes, the risk profiles and proposed mitigations may need to be reevaluated to ensure they reflect the current state of risk to the DNS and Internet routing critical functions.

13 Appendix

Since the conclusion of the latest assessment, there have been additional materials released that are related or complementary to the information in this report. The following is a list of links to additional reading materials and references that may assist the reader in conducting an organizational risk assessment related to DNS and Internet Routing.

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure, May 11, 2017. < https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>

National Institute for Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*, <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

NIST Cybersecurity Framework – Updates. <https://www.nist.gov/cyberframework>

Department of Homeland Security - U.S. Computer Emergency Readiness Team (CERT) Cybersecurity Framework Functional Areas Stakeholder Engagement and Critical Infrastructure Resilience (SECIR) Cyber Resilience Review. <https://www.us-cert.gov/ccubedvp/assessments>

NIST Special Publication 800-81-2 Secure Domain Name System (DNS) Deployment Guide. <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf>