ICANN

DNS Security and Stability Analysis Working Group (DSSA)

Phase 1 Report

15-June, 2012

1. Executive Summary

This is the first of two reports from the DNS Security and Stability Analysis working group. The goal of this document is to bring forward the substantial work that has been completed to date and describe the work that remains.

This has been in many respects a "pioneering" cross-constituency security-assessment effort that has developed knowledge and processes that others will hopefully find helpful and can be reused in the future.

The DSSA has:

- Established a cross-constituency working group and put the organizational framework to manage that group in place
- Clarified the system, organizational and functional scope of the effort
- Developed an approach to handling confidential information, should such information be required for certain assessments
- Selected and tailored a risk-assessment methodology to structure the work
- Developed and tested mechanisms to rapidly collect and consolidate risk-assessment scenarios across a broad and diverse group of interested participants
- Used an "alpha-test" of those systems to develop the high-level risk-scenarios in this report. Those scenarios will serve as the starting point for the remainder of the effort

Work that remains:

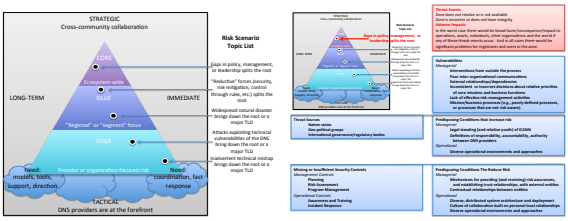
- Perform a proof of concept to refine and streamline the methodology on one broad risk-scenario topic with the goal of reducing cycle time and making it more accessible to a broader community
- Roll the methodology out to progressively broader groups of participants to introduce the methodology to the community and further improve the process and tools on the way to completing the assessment

1.1. Key findings

The DSSA has a number of observations to share with the community after completing the first phase of its work. Those observations are summarized here, presented in more detail in the body of this report and in some cases presented in even more detail in the Appendix. The working group has also developed a series of tools that can be used by any DNS provider to conduct risk

assessments. Those tools, and extremely detailed documentation of the assessment, are available on the working group wiki.

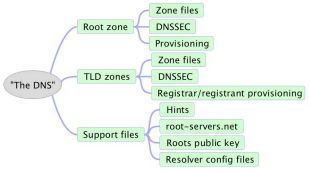
1.1.1. Risk Scenarios

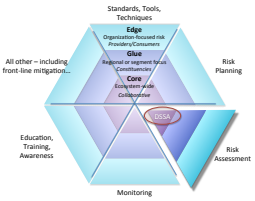


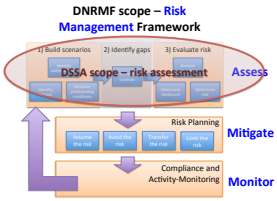
The DSSA has analyzed five broad risk scenarios. These will be explored in more depth during the next phase of the effort. Those scenarios are:

- Gaps in policy, management, or leadership lead to splitting the root
- "Reductive" forces (security, risk-mitigation, control through rules, etc.) lead to splitting the root
- Widespread natural disaster brings down the root or a major TLD
- Attacks exploiting technical vulnerabilities of the DNS bring down the root or a major TLD
- Inadvertent technical mishap brings down the root or a major TLD

1.1.2. Scope



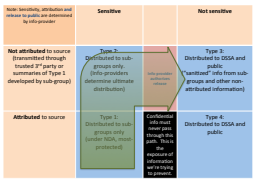


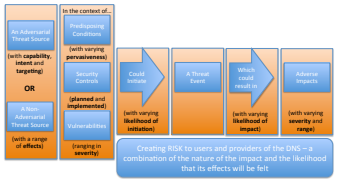


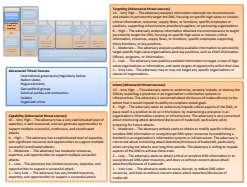
The DSSA analyzed several scope issues that needed to be resolved in order to complete the work.

- Scope of "the DNS" used by the working group
- The functional context of the DSSA within a broader risk management framework
- The organizational context of the DSSA vis a vis the SSR-RT and DNRMF efforts

1.1.3. Approach



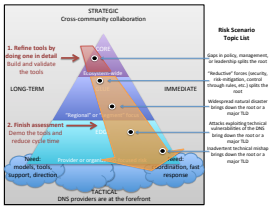


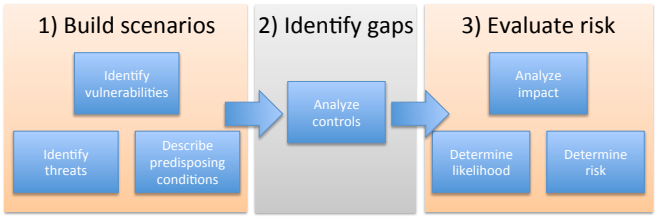


The DSSA also embarked on developing methodologies that were required in order for the working group to complete its assignments. These methods may be useful in other contexts, both inside and outside of ICANN. These include:

- A protocol for handling confidential information
- A tailored "compound sentence" risk-assessment methodology based on the NIST 800-30 and 800-53 standards
- An approach to risk assessment that accommodates the unique security assessment requirements of the multi-stakeholder DNS ecosystem

1.1.4. Remaining work





The DSSA realized that a detailed assessment of the risk scenarios it has identified is likely to take a substantial amount of time. The DSSA, after consultation with its chartering ACs and SOs, broke its work into two phases. This report summarizes the work to date, while the next phase will:

- Take that work to a more detailed level,
- Refine the approach and methods developed so far, and
- Explore whether it is feasible to transition this one-time effort into an ongoing function to maintain an up to date assessment of DNS risk.

2. Background, Charter and Scope

2.1. Background

From the DSSA Charter:

> At their meetings during the ICANN Brussels meeting in June 2010, the At-Large Advisory Committee (ALAC), the Country Code Names Supporting Organization (ccNSO), the Generic Names Supporting Organization (GNSO), the Governmental Advisory Committee (GAC), and the Number Resource Organization (NROs) **acknowledged the need for a better understanding of the security and stability of the global domain name system (DNS)**. This is considered to be of common interest to the participating Supporting Organisations (SOs), Advisory Committees (ACs) and others, and should be preferably undertaken in a collaborative effort.
>
> To this end the ALAC, ccNSO, GNSO and NRO agreed to establish a Joint DNS Security and Stability Analysis Working Group (DSSA-WG), in accordance with each own rules and procedures and invite other AC's to liaise and engage with the DSSA-WG in a manner they consider to be appropriate.

2.2. Charter, Scope and Approach

2.2.1. Objectives and Goals

From the DSSA Charter:

> The objective of the DSSA-WG is to draw upon the collective expertise of the participating SOs and ACs, solicit expert input and advice and report to the respective participating SOs and ACs on:
>
> A. The actual level, frequency and severity of threats to the DNS;
> B. The current efforts and activities to mitigate these threats to the DNS; and
> C. The gaps (if any) in the current security response to DNS issues.
>
> If considered feasible and appropriate, the DSSA-WG may identify and report on possible additional risk mitigation activities that it believes would assist in closing any gaps identified under item C above.
>
> Each of the participating SOs and ACs has adopted this charter according to its own rules and procedures.

2.2.2. Scope

From the DSSA Charter:

The DSSA-WG should limit its activities to considering issues at the root and top level domains within the framework of ICANN's coordinating role in managing Internet naming and numbering resources as stated in its Mission in its Bylaws. The DSSA-WG also should take into account and attempt to coordinate with existing, ongoing, and emerging research, studies, and initiatives with respect to the DSSA-WG objectives. Subject to the limitations above, the DSSA-WG should do whatever it deems relevant and necessary to achieve its objectives."

The DSSA had to refine and clarify its scope in three dimensions in order to complete its work;

- The scope boundaries of "the DNS" (sometimes called "**system boundaries**"),
- The **functional** scope of the effort in the context of a much broader "Security Management" function (which has ICANN-specific elements and broader "DNS" components), and
- The **organizational** context of the effort (the DNS "ecosystem" and the Board DNS Risk Management Framework working group).

2.2.2.1. Scope of "the DNS" used by the DSSA working group

The DSSA charter states that the working group is to review: "The actual level, frequency and severity of threats to the DNS" but leaves the definition of "the DNS" up to the working group. However the charter offers the following additional guidance. "The DSSA-WG should limit its activities to considering issues at the root and top level domains within the framework of ICANN's coordinating role in managing Internet naming and numbering resources as stated in its Mission and in its Bylaws."

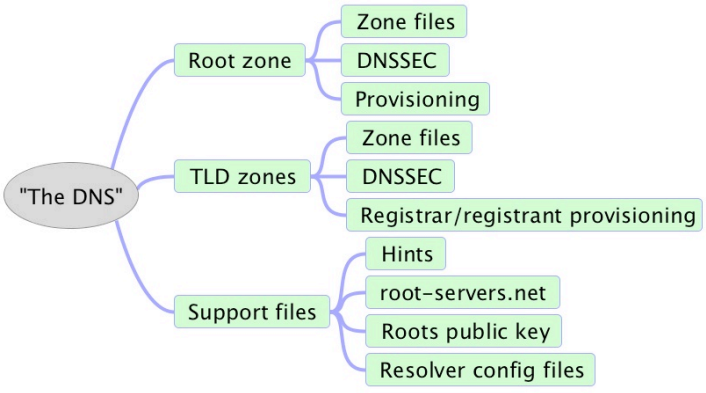


Figure 1

"The DNS" includes:

- The Root zone (zone files, DNSSEC and provisioning)
- Top-level domain zones (zone files, DNSSEC and provisioning)
- Support files (e.g. hints, root-servers.net, roots public key, resolver configuration files

Out of scope of this analysis

- 2nd-level zones and lower
- WHOIS
- Zone file access
- Data escrow
- Bulk data access

Observations

- The working group arrived at the above definition of "The DNS" for the purposes of this analysis. It needs to be emphasized that this definition is primarily aimed at structuring the work to be done within the limits set by the charter. Broader use of this definition of "the DNS" within the community should be undertaken with caution.

- There is unanimous consensus within the DSSA that this is the appropriate definition of "The DNS" for its work – but particular attention should be paid to those items that were deemed out of scope for this analysis. The DSSA encourages the community to analyze security risks in those areas as well, but for the purpose/charter of this working group they are deemed either not part of the core DNS system, or they fall outside the ICANN remit.

2.2.2.2. DSSA scope – functional context

The DSSA describes its (quite narrow) relationship to the broader DNS security "ecosystem" in two dimensions – it's relationship with day-to-day front-line DNS-delivery and security management (the "core" to "edge" relationship in the diagram below) and the functional scope of its effort (the "spokes" or pie-slices of the diagram).

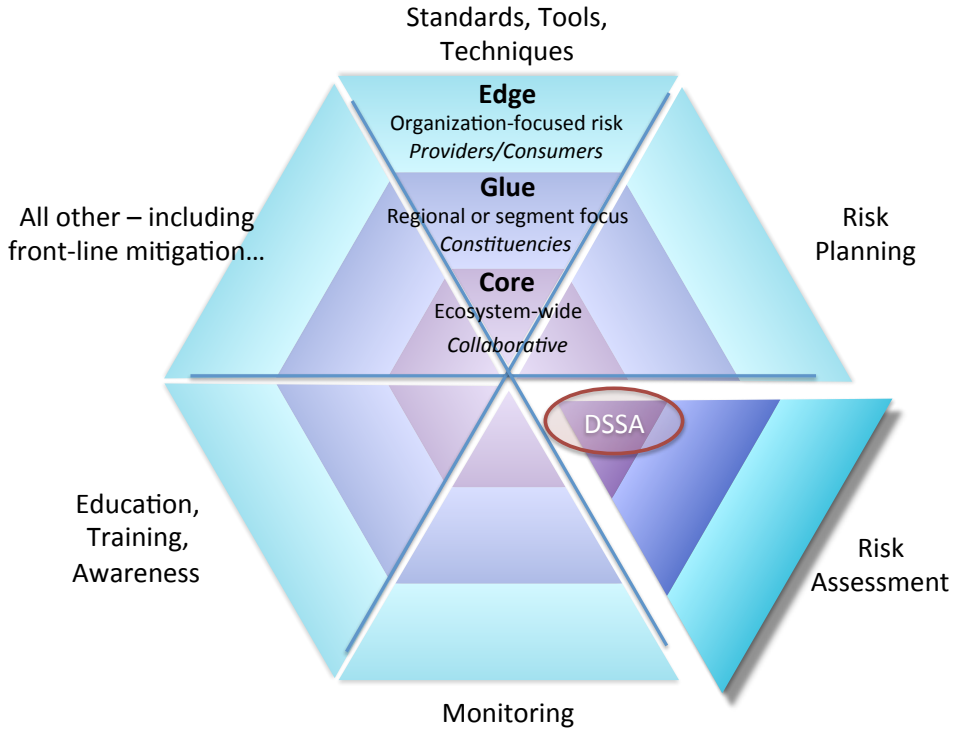


Figure 2

Observations

- This is a working diagram that the DSSA developed in order to refine and focus its effort. It should not be viewed as a recommendation – recommendations about the structure of the risk-management and security-management framework are outside our remit and being developed by others. But the DSSA began working before broader efforts such as the SSR-RT and the DNRMF produced their recommendations and the team needed an interim working definition in order to describe the scope boundaries of its effort.

- A useful exercise would be to array other organizations that have a role in DNS security on a diagram such as this one, partly to highlight the number of participants and partly to identify gaps and overlaps. Here is a partial list:

  - Backend registry providers
  - ccTLD registries
  - CERTs
  - DNS-OARC
  - ENISA
  - FIRST
  - gTLD registries
  - IANA
  - ICANN Security Team
  - ICANN SOs and ACs

- IETF
- ISOC
- Network Operator Groups
- NRO
- RSAC
- SSAC
- SSR-RT
- DNRMF

- If a model like this were adopted, information and knowledge could flow in both directions core to edge and edge to core. Constituencies and other "glue" organizations could be the means by which this happens – if they know that's their role and can support the activity.

- The collaborative core could be where information is exchanged and shared-direction is described. The front-line edge could be where; delivery-authority resides, new ideas are applied, lessons are learned, and those lessons are summarized and passed back to the core.

- There is room for more components of risk-management in this model. The ones that are listed can be viewed as a starting point for discussion. But no matter what portfolio is eventually put in place, efforts like the DSSA will be more effective when the rest of the functions are better developed. For example:

    - DSSA-like efforts may be somewhat starved for information until some kind of shared audit and compliance capability is in place (largely at the edge). Risk assessment efforts (especially in the multi-stakeholder context) have a very delicate line to tread when inquiring into security incidents across organizational boundaries. Future teams would find it much easier to complete their work if it was based on the lessons learned, and reflected in, data generated by others rather than developing the data within the project.

    - Assessments would likely be of more value if they could be used to incrementally shape and improve an existing body of risk-related standards, tools and techniques. Similarly, those techniques could be made more useful if they could be rapidly and effectively shared and subjected to the test of front-line reality.

    - All of this works better if it is done in the context of a risk plan that suggests how to respond to the risks that are being identified. A DSSA-like effort benefits from an audience that can turn its observations into action-plans – a "risk planning" function could be a good place to start.

- There are different roles for "ICANN the corporation" and "ICANN the community." The corporation has largely front-line DNS work to do while "the community" forms part of the core and glue layers (and is supported by "ICANN the corporation" which sometimes leads to confusion and role conflicts). Clarifying these roles and responsibilities would be helpful for all participants, not just the DSSA. Indeed the recent report from the SSR-RT suggests that clarifying those roles would improve security and stability of the DNS.

The following diagram highlights how narrow the role of the DSSA is when compared to the range of activities addressed by a traditional "Security Management" function in a technical systems organization. This is the context of the DSSA when viewed from the perspective of "the edge."

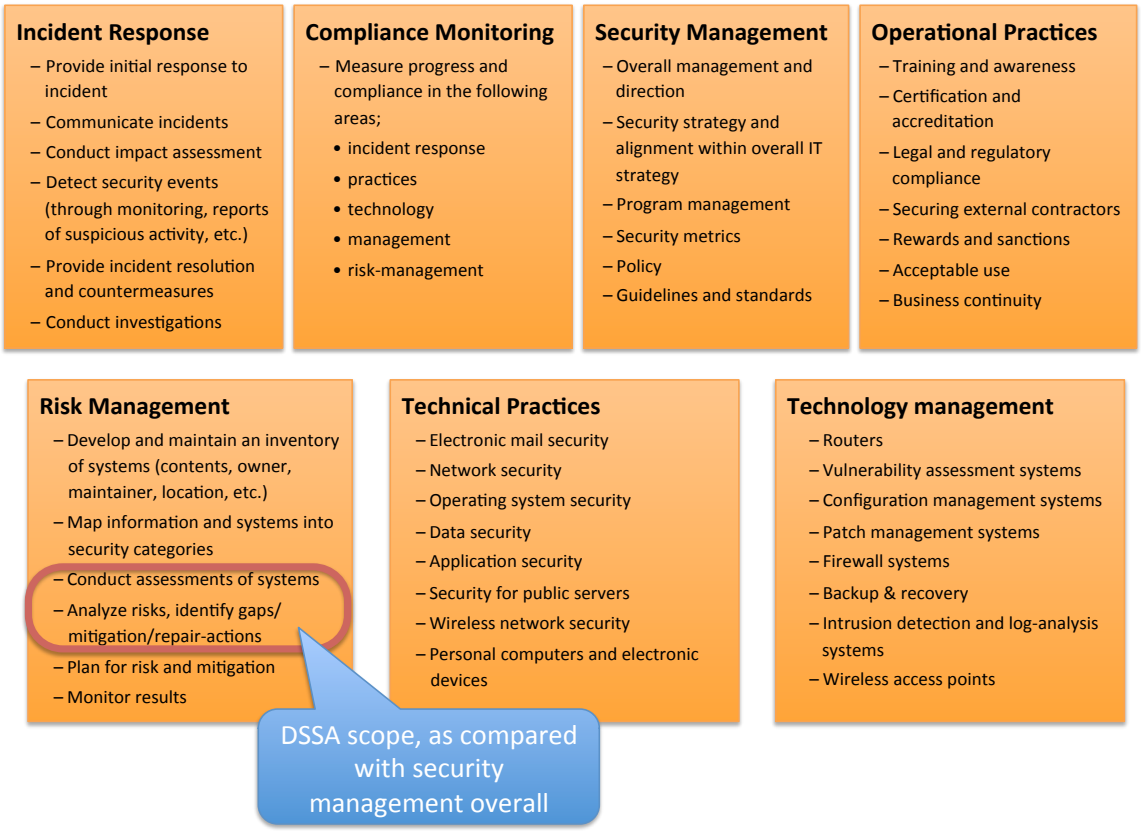


Figure 3

Observations

- Each DNS provider "at the edge" probably has some form of all of these activities happening now – with widely varying needs, focus, capability and so forth. "ICANN the corporation" in its front-line DNS-root delivery role certainly does. The DSSA cannot possibly replace that internal capability, nor can it take on the many other operational security functions that are represented here.

- Future DSSA-like efforts may be better focused on developing tools and techniques to assess "threats to the DNS" that can be shared among the very diverse community of front-line DNS providers, rather than attempting to do a single assessment that encompasses them all.

2.2.2.3. DSSA scope – organizational context

This last discussion about the scope of the DSSA describes the relationship between the DSSA and the ICANN-Board DNS Risk Management Framework Working Group (DNRMF WG). Again, this model, and the observations that follow, should not be viewed as recommendations (indeed

describing the risk-management framework is precisely what the DNRMF is chartered to do) but rather as a mechanism to put scope-boundaries on the DSSA effort while that framework is being established.

2.2.2.3.1. Relationship to the ICANN-Board DNS Risk Management Framework Working Group (DNRMF WG)

The DNS Risk Management Framework Working Group (DNRMF WG) states:

> "The ICANN Board has asked (2011.03.18.07) the Board Governance Committee to recommend to the Board a working group to oversee the development of a risk management framework and system for the DNS as it pertains to ICANN's role as defined in the ICANN Bylaws.
>
> The purpose of the DNS Risk Management Framework WG (DNRMF WG) is to **develop goals and milestones towards the implementation of a DNS security risk management framework for Internet naming and address allocation services, accompanied by defined timelines and budgetary implications. Further, the DNRMF WG will oversee the creation of an initial assessment which will serve as a baseline for the task."**

The diagram that follows describes the "risk management" portion of the "circle diagram" that was discussed previously. The DSSA used this model to describe the functional boundary of its effort and to highlight its narrow "risk assessment" duties as they relate to the broader "risk management" function.

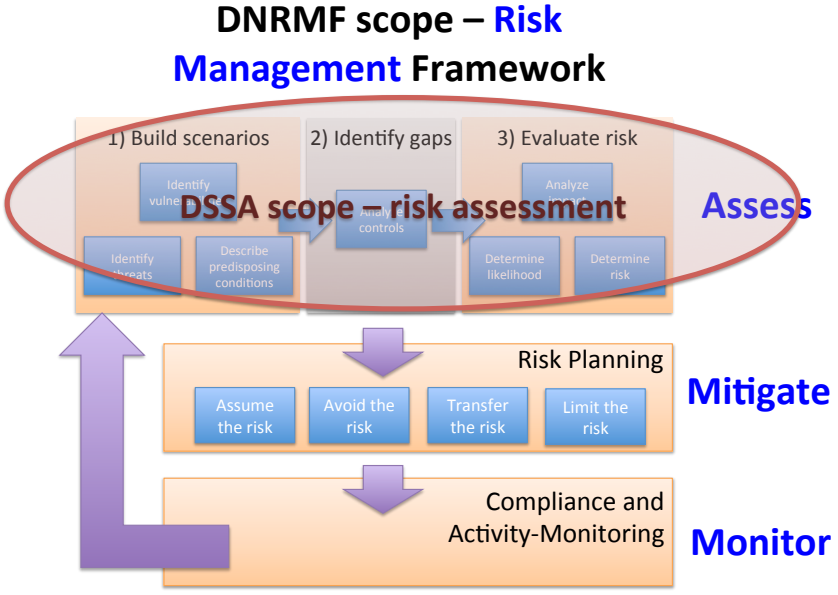


Figure 4

Observations

- Note the distinction between "risk assessment" (which is what the DSSA is chartered to do) and "risk management" (which is a broader topic that includes, but is not limited to, risk assessment)

- Also note that the DSSA charter is to **do** a risk-assessment – the DNRMF charter is to develop goals and milestones to **establish** a risk-management framework, **and** oversee a baseline initial assessment. Thus the scope of the DNRMF is different in several dimensions:

    - The function the DNRMF is charged with defining is broader (including mitigation and monitoring functions in addition to assessment).

    - The deliverables of the DNRMF include both defining the functions **and** conducting a baseline assessment once that definition is established.

    - The framework the DNRMF is selecting is presumably the beginning of an ongoing security management process whereas the DSSA is chartered as a one-time assessment.

- While the DSSA is narrower, the assessment (and assessment methods) developed by the DSSA may prove useful contributions to the work of the DNRMF.

- In a perfect world, the whole risk-management framework – assessment, mitigation and monitoring – would have been in place before the DSSA began its work. Because it was not the DSSA could only assess based on the personal knowledge and experience of its participants in this first cycle. It was also difficult to evaluate controls when the risk-mitigation strategy has yet to be defined.

- An assessment based on data, that measures the alignment of current practices with an overall risk-mitigation approach, will have to wait until those mitigation and monitoring capabilities have been defined and put in place. Once that is done, the "assessment" group could then base its analysis on broader and deeper data coming out of the monitoring cycle and determine how well existing controls align with risk-mitigation strategy.

- Given that the DSSA was launched before this broader framework was in place, the group needed to select and tailor a risk-assessment methodology in order to complete its work. The methods and models that have been developed may prove to be a useful contribution to the broader risk-management work of the DNRMF – but it should not be considered preemptive.

2.2.3. Analysis approach

The working group has tailored NIST methodologies (800-30 risk-assessment and NIST 800-53a controls-assessment) into a series of steps to build "compound-sentence" risk scenarios that define the starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated.

While not a part of its charter, the working group needed to define a risk assessment framework in order to complete its work. That framework is being built with the hope that more specialized teams (and other organizations) can use it in the future to develop additional scenarios or analyze already-identified scenarios in more depth. The methods are being continuously refined to reduce cycle-time with the goal that it may some day be possible to go through the whole process very quickly (perhaps as quickly as an hour or less), thus making it useful to a first-responder team in addition to addressing the typically much longer timeframes of a policy-making group.

The diagram that follows illustrates the assessment process at a very high level and highlights the three stages of the assessment for a given risk topic.

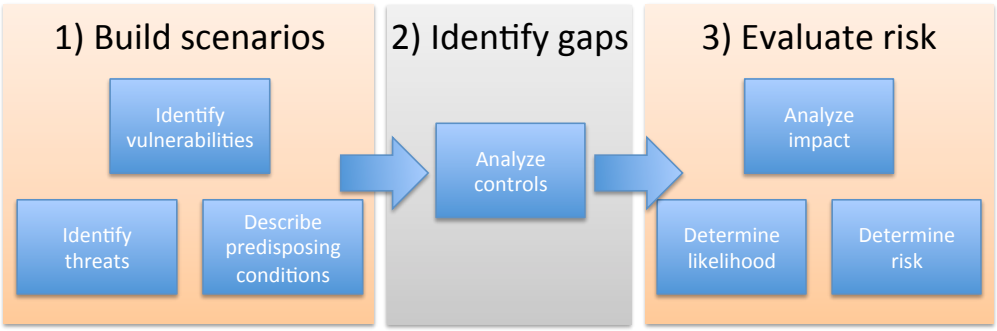


Figure 5

Step 1 – Build Scenarios

Use risk-scenario worksheets to quickly brainstorm a series of related scenarios based on the broad risk topic under discussion.

Step 2 – Identify gaps

Use a structured survey process to collectively evaluate each threat-scenario (threat-events, vulnerabilities and predisposing conditions) and then identify and evaluate gaps in security controls.

Step 3 – Evaluate risk

Use a structured survey process to collectively evaluate the risk of each threat-scenario

3. Findings

3.1. Overview

This section describes (at a very high level) the work-products and findings of this first ("go fast") phase of the work. Here is a severely edited summary of a much larger body of work that has been relegated to the Appendices in order to constrain this report to a reasonable length.

3.2. Work products

Some members of the DSSA working group burst into hysterical laughter at the "go fast" description of this phase of the work. After all, the need for this effort was identified almost exactly two years ago at the ICANN meeting in Brussels. But this has been in many respects a "pioneering" effort that has hopefully developed processes that others will find helpful and can be reused in the future.

The DSSA effort has:

- Established a cross-constituency working group and put the organizational framework to manage that group in place
- Clarified the system, organizational and functional scope of the effort
- Developed an approach to handling confidential information, should such information be required for certain assessments
- Selected and tailored a risk-assessment methodology to structure the work
- Developed and tested mechanisms to rapidly collect and consolidate risk-assessment scenarios across a broad and diverse group of interested participants
- Used an "alpha-test" of those systems to develop the high-level risk-scenarios in this report. Those scenarios will serve as the starting point for the remainder of the effort

Work that remains:

- Perform a proof of concept to refine and streamline the methodology on one broad risk-scenario topic with the goal of reducing cycle time and making it more accessible to a broader community
- Roll the methodology out to progressively broader groups of participants to introduce the methodology to the community and further improve the process and tools on the way to completing the assessment

3.3. Current state of the assessment of "The actual level, frequency and severity of threats to the DNS, plus current efforts and activities to mitigate these."

The title of this section comes directly from the DSSA Charter and is viewed by working-group members as the first of three key findings that needs to come out of the effort. The diagram that follows places a preliminary series of five broad risk scenarios (that the DSSA will develop in more detail during the next portion of its work) along several dimensions.

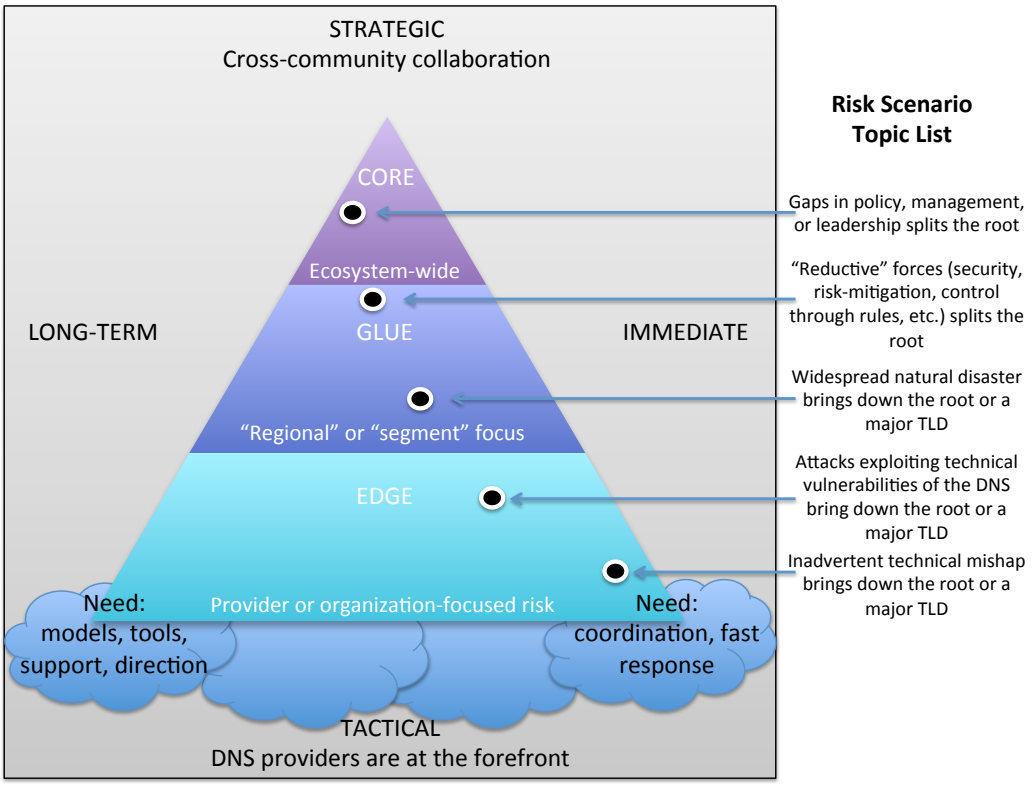


Figure 6

- **Gaps in Policy, Management, Leadership Lead to Splitting the Root**

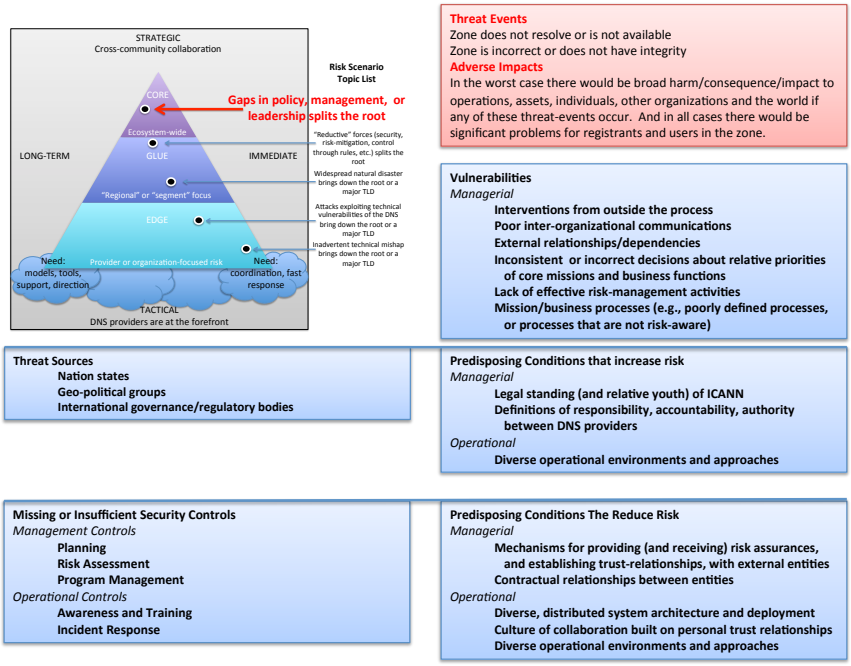


Figure 7

- **"Reductive" Forces (Security, Risk-mitigation, Control through rules, etc.) Lead to Splitting the Root**

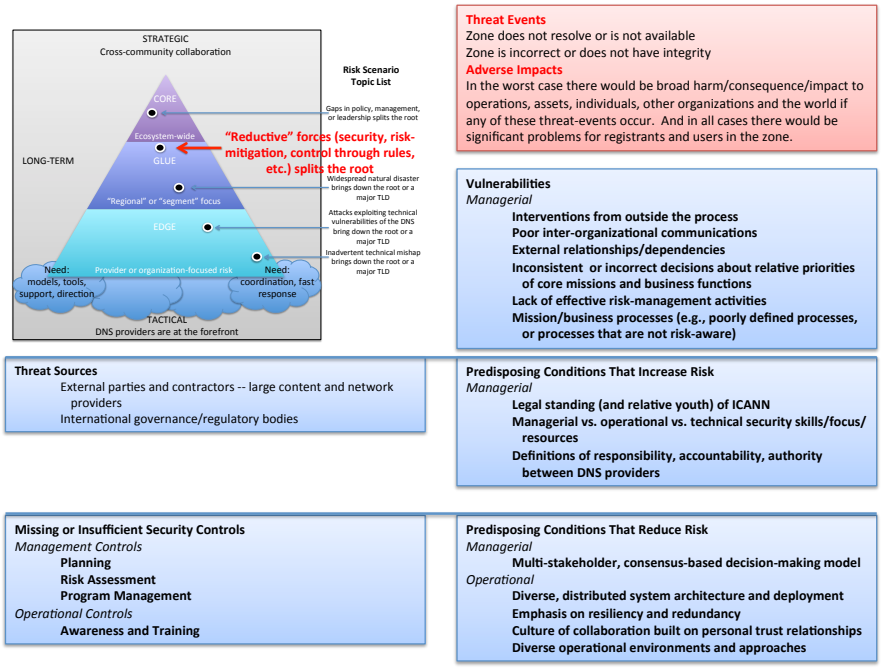


Figure 8

- **Widespread Natural Disaster Brings Down the Root or a Major TLD**

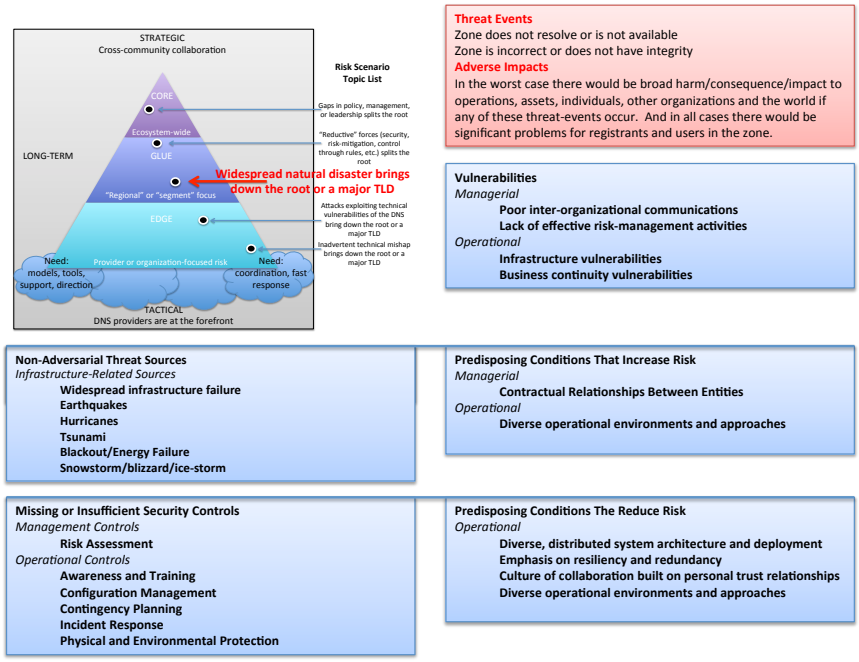


Figure 9

- **Attacks Exploiting Technical Vulnerabilities of the DNS Bring Down the Root or a Major TLD**

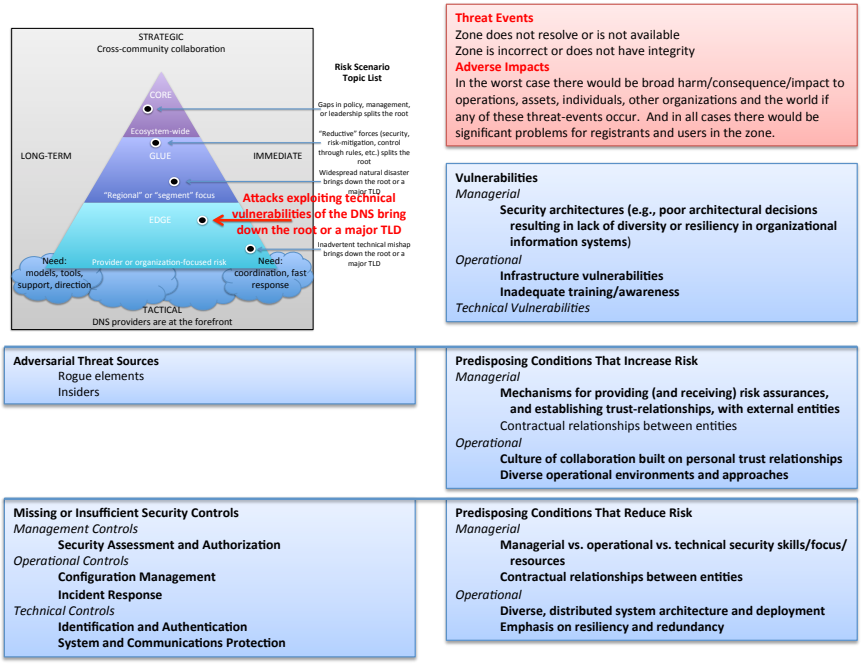


Figure 10

- **Inadvertent Technical Mishap Brings down the Root or a Major TLD**

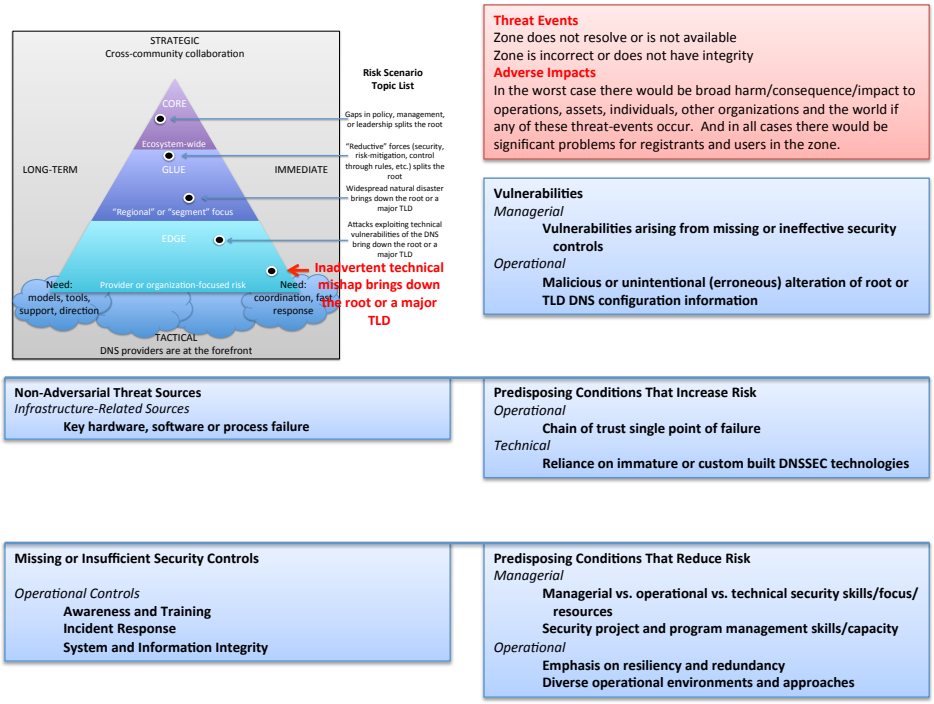


Figure 11

Larger versions of these charts are available in the Appendix

Observations

- These topics outline the shape of the analysis and can be viewed as the preliminary topic-list that the DSSA will use to guide its work as it "goes deep" into at least one topic during the next phase of the work.

- These topics should not be viewed as anything but working drafts at this stage of the analysis. Sharp-eyed readers will note a number of inconsistencies in these topics as presented here.

- Pay particular attention to the underlying dimensions of the model. The DSSA is coming to realize that one size does not fit all in this analysis.

    - Issues that are very important to the strategically focused "core" participants are likely to differ substantially from those impacting organizations at the front-line "edge."

    - Also note the difference in timeframe – certain kinds of risks evolve much more slowly than others, which needs to be taken into account when conducting the analysis.

The DSSA is especially interested in hearing from the community as to whether it has missed any major risk-scenarios. Please review this list with that request in mind and consider forwarding your suggestions to the DSSA directly.

If you are concerned that simply describing a particularly embarrassing scenario might reveal confidential information about you or your organization, Paul Vixie (paul@vix.com) has volunteered to act as an intermediary to enter into a confidentiality agreement with you and "anonymize" your suggestion. Contact information for the DSSA and Paul is contained in the Appendix.

3.4. Current state of the assessment of the remaining charter-questions

The DSSA charter asks three additional questions:

- "What are the current efforts and activities to mitigate these threats to the DNS?"
- "What are the gaps (if any) in the current security response to DNS issues?"
- "If considered feasible and appropriate, what additional risk mitigation activities would assist in closing any gaps identified above?"

Arriving at the answers to these questions must, for the most part, wait until the next phase of the work and may in fact have to wait until some of the other components of the Risk Management Framework are in place (see "Scope" section above).

Observations

- The DSSA notes that there are several factors that may make it very difficult to arrive at a single unified answer to the questions posed in its charter:
    - Answers vary with the nature of the DNS-provider (e.g. root-server operators, gTLD server operators, ccTLD server operators, ICANN, etc.)
    - Answers also vary with the scale and maturity of the provider, as well as the scope and "attractiveness to adversaries" of the information they serve
    - Answers change over time – more rapidly for immediate/tactical threats to the "edge" vs. those which are strategic risks
- The DSSA hopes to refine its risk-assessment processes to a point where the many DNS providers in the ecosystem can some day collectively develop an ongoing series of coordinated risk-assessments, each from their own perspective. It is further hoped that these can be summarized in a way that they can be made broadly accessible to the community. In the long term these independent assessments might be combined to arrive at the "current state of DNS security" overview that is implied in the DSSA charter.
- This is not to say that the DSSA plans to leave its work incomplete, only to set appropriate expectations. The DSSA risk assessment will be largely based on the knowledge of its members, which is a very diverse, expert and well-informed group. But future assessments will benefit greatly from more mature risk-management that includes:
    - Risk-strategy (determining appropriate risk-mitigation strategies which can then be used as the basis for gap analysis) and
    - Structured information gathering (self-audit and compliance functions) that can produce much more detailed and accurate information upon which to base the assessments.

- The DSSA coordinated its work with that of the Security, Stability and Resiliency of the DNS Review Team (SSR-RT) chartered under the Affirmation of Commitments and notes that a number of the recommendations flowing from that effort will, if implemented, greatly improve the effectiveness of DSSA-like efforts in the future Copies of the SSR-RT report can be found at the Public Comment forum -- http://www.icann.org/en/news/public-comment/ssrt-draft-report-15mar12-en.htm What follows is a list of the SSR-RT recommendations (as of this writing) that most directly bear on the DSSA gap-assessment and future-improvements charter questions.
    - Recommendation 1: ICANN should publish a single, clear and consistent statement of its SSR remit and limited technical mission. ICANN should elicit and gain public feedback in order to reach a consensus-based statement.
    - Recommendation 3: ICANN should document and clearly define the nature of the SSR relationships it has within the ICANN community in order to provide a single focal point for understanding the interdependencies between organizations.
    - Recommendation 4: ICANN should use the definition of its SSR relationships to encourage broad engagement on SSR matters using this to create an effective and coordinated SSR approach.
    - Recommendation 12: ICANN should support the development and implementation of SSR-related best practices through contracts, agreements, MOUs and other mechanisms.
    - Recommendation 13: ICANN should encourage all Supporting Organizations to develop and publish SSR related best practices for their members.
    - Recommendation 14: ICANN should ensure that its SSR related outreach activities continuously evolve to remain relevant, timely and appropriate. Feedback from the community should provide a mechanism to review and increase this relevance.
    - Recommendation 15: ICANN should publish information about DNS threats and mitigation strategies as a resource for the broader Internet community.
    - Recommendation 16: ICANN should continue its outreach efforts to expand community participation and input into the SSR Framework development process. ICANN also should establish a process for obtaining more systematic input from other ecosystem participants.
    - Recommendation 23: ICANN must provide appropriate resources for SSR-related working groups and advisory committees, consistent with the demands place upon them. ICANN also must ensure decisions reached by working groups and advisory committees are reached in an objective manner that is free from external or internal pressure.

4. Approach to the work, this phase and in the future

4.1. Approach – A hybrid of "go fast, then go deep" for the DSSA, perhaps followed by an ongoing effort after the DSSA and DNRMF complete their work

The DSSA consulted with the community towards the end of this first phase of its work after realizing that the scope of a detailed risk assessment might result in an effort that could last several years. The question that was posed was "which is preferable, quick or detailed results?" to which the answer from the community was "yes, we see value in both approaches."

Thus, the DSSA has split its work into two phases. This first "go fast" phase will conclude with the publication of this report, after a public comment cycle. The second "go deep" phase will take the assessment one level deeper, test and refine the methods that have already been developed, and test some approaches to broadening participation in the assessment among the DNS-provider community.

The DSSA observes that there is a need for ongoing risk assessment of the DNS. The DSSA is chartered as a cross-constituency working group within ICANN that will end soon and is not an entity that can organize or deliver this kind of permanent capability. However the DSSA has several observations about ongoing DNS risk assessment that the community may find helpful as it decides whether to organize and deliver that capability.

Here is a brief summary of the two phases of the DSSA effort;

Phase 1 – "go fast"

- Establish a cross-constituency working group and put the organizational framework to manage that group in place
- Clarify the system, organizational and functional scope of the effort
- Develop an approach to handling confidential information, should such information be required for certain assessments
- Select and tailor a risk-assessment methodology to structure the work
- Develop and test mechanisms to rapidly collect and consolidate risk-assessment scenarios across a broad and diverse group of interested participants
- Use an "alpha-test" of those systems to develop the high-level risk-scenarios for the Phase 1 report. Those scenarios will serve as the starting point for the remainder of the effort
- Solicit public comment on the work to date and incorporate those suggestions into the plans for the next phase.

Phase 2 – "go deep"

- Perform a proof of concept to refine and streamline the methodology on one broad risk-scenario topic with the goal of reducing cycle time and making it more accessible to a broader community.
- Roll the methodology out to progressively broader groups of participants to introduce the methodology to the community and further improve the process and tools.
- Report the results of those more-detailed assessments to the community, solicit comments, and incorporate those comments into the final report.

4.2. During this "go fast" iteration

The "go fast" phase of the DSSA produced several substantial "process" deliverables that are briefly summarized here and documented in detail in the Appendices. The DSSA hopes that this documentation will be of use to others in the ecosystem.

Observations

- Future teams would greatly benefit from a well-maintained, up to date repository, of risk-management resources that could be used as a starting point for many of these activities. Simply researching (or creating) the documents used to build the work products described in this section drew an extraordinary amount of working-group time and attention away from its "conduct an assessment" task.
- It is beyond the remit of this working group to recommend where this resource library should reside in the ecosystem, but suggests that this effort could be very low cost, provide tremendous benefits across the community, and does not represent much in the way of continual scope expansion (or "scope creep") to any organization that elects to take it on.
- Conversely, it can be argued that leaving each security-management working group to discover or invent security-management techniques on their own increases overall risk to the DNS by making risk-responders and managers much less effective.

4.2.1. Methods – rationale, selection, risk model and tailoring

Perhaps the most important intermediate work product of the DSSA was the selection and tailoring of a risk-assessment methodology. The process by which that methodology was selected and tailored to meet the unique needs of the ICANN community are summarized here and detailed in the Appendix.

Rationale

The DSSA concluded several months into the effort that it was floundering. The group decided that using a predefined methodology would save time and improve its work product by providing

consistent terminology, a proven model and structure for the work, and sample work plans and deliverables.

The DSSA selected the NIST 800 series methods, after reviewing several dozen options, because it is available at no cost, actively supported and maintained, widely known and endorsed, and may be reusable elsewhere in the community.

4.2.2. Risk assessment framework

The DSSA initially struggled to use NIST 800-30 in its unmodified form and eventually tailored the methodology to a point that was much more useful to the working group while still remaining true to the essence of the methodology. The "compound sentence" framework developed by the DSSA is summarized in this diagram and documented in detail in the Appendix.

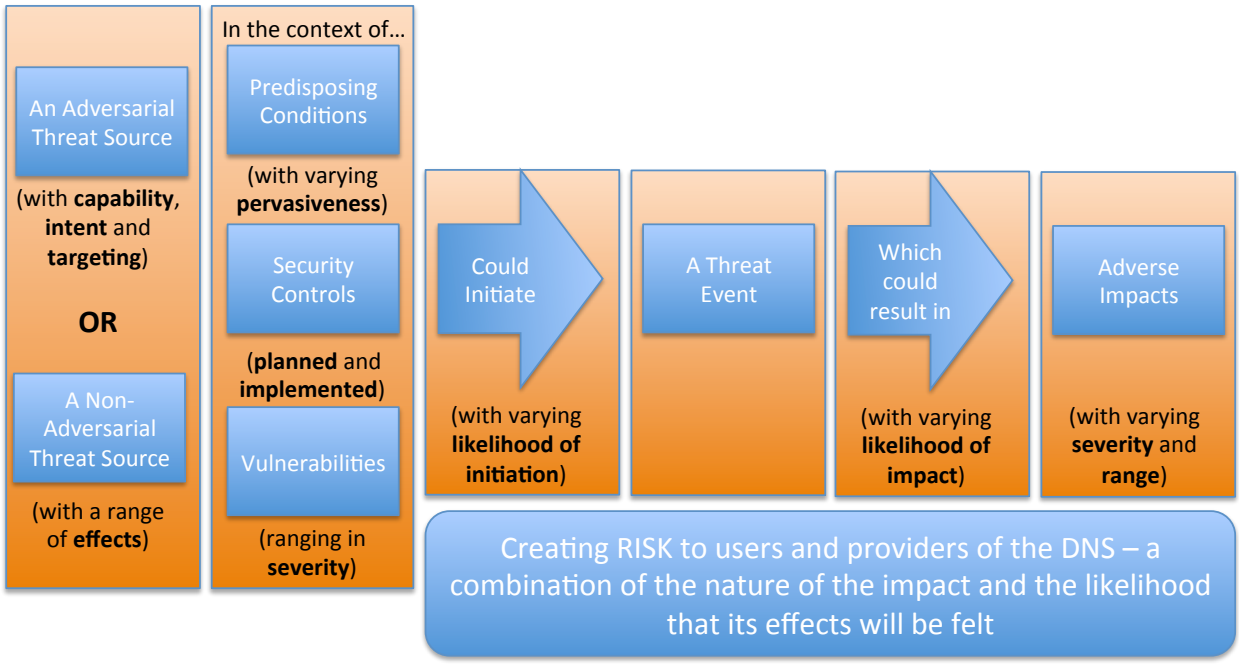
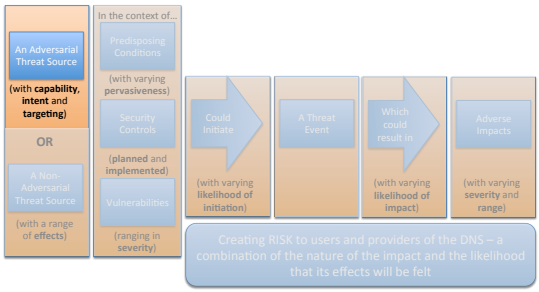


Figure 12

"An <u>Adversarial Threat Source</u> (with capability, intent and targeting)…



Adversarial Threat Sources

International governance/regulatory bodies
Nation states
Rogue elements
Geo-political groups
External parties and contractors
Insiders
Organized crime

Capability (Adversarial threat sources)

10 -- Very High -- The adversary has a very sophisticated level of expertise, is well-resourced, and can generate opportunities to support multiple successful, continuous, and coordinated attacks.

8 -- High -- The adversary has a sophisticated level of expertise, with significant resources and opportunities to support multiple successful coordinated attacks.

5 -- Moderate -- The adversary has moderate resources, expertise, and opportunities to support multiple successful attacks.

2 -- Low -- The adversary has limited resources, expertise, and opportunities to support a successful attack.

1 -- Very Low -- The adversary has very limited resources, expertise, and opportunities to support a successful attack

Targeting (Adversarial threat sources)

10 -- Very High -- The adversary analyzes information obtained via reconnaissance and attacks to persistently target the DNS, focusing on specific high-value or mission-critical information, resources, supply flows, or functions; specific employees or positions; supporting infrastructure providers/suppliers; or partnering organizations.

8 -- High -- The adversary analyzes information obtained via reconnaissance to target persistently target the DNS, focusing on specific high-value or mission-critical information, resources, supply flows, or functions, specific employees supporting those functions, or key positions.

5 -- Moderate -- The adversary analyzes publicly available information to persistently target specific high-value organizations (and key positions, such as Chief Information Officer), programs, or information.

2 -- Low -- The adversary uses publicly available information to target a class of high-value organizations or information, and seeks targets of opportunity within that class.

1 -- Very Low -- The adversary may or may not target any specific organizations or classes of organizations.

Intent (Adversarial threat sources)

10 -- Very High -- The adversary seeks to undermine, severely impede, or destroy the DNS by exploiting a presence in an organization's information systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede its ability to complete stated goals.

8 -- High -- The adversary seeks to undermine/impede critical aspects of the DNS, or place itself in a position to do so in the future, by maintaining a presence in an organization's information systems or infrastructure. The adversary is very concerned about minimizing attack detection/disclosure of tradecraft, particularly while preparing for future attacks.

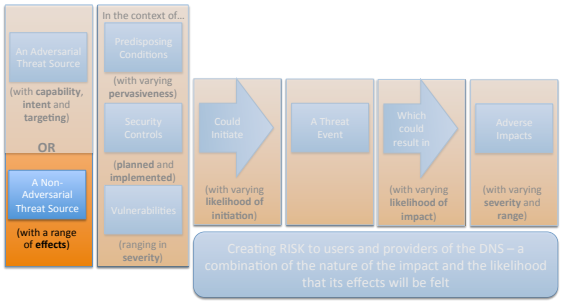
5 -- Moderate -- The adversary actively seeks to obtain or modify specific critical or sensitive DNS information or usurp/disrupt DNS cyber resources by establishing a foothold in an organization's information systems or infrastructure. The adversary is concerned about minimizing attack detection/disclosure of tradecraft, particularly when carrying out attacks over long time periods. The adversary is willing to impede aspects of the DNS to achieve these ends.

2 -- Low -- The adversary seeks to obtain critical or sensitive DNS information or to usurp/disrupt DNS cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

1 -- Very Low -- The adversary seeks to usurp, disrupt, or deface DNS cyber resources, and does so without concern about attack detection/disclosure of tradecraft.

Figure 13

OR a <u>Non-Adversarial Threat Source</u> (with a range of effect)…"



Non-Adversarial Threat Sources

Individual And Organizational Sources

- International governance/regulatory bodies
- Nation states
- Privileged users
- Key providers

Root-Related Sources

- Alternate DNS roots
- Root scaling (SAC 46)
- Intentional or accidental results of DNS blocking (SAC 50)

Infrastructure-Related Sources

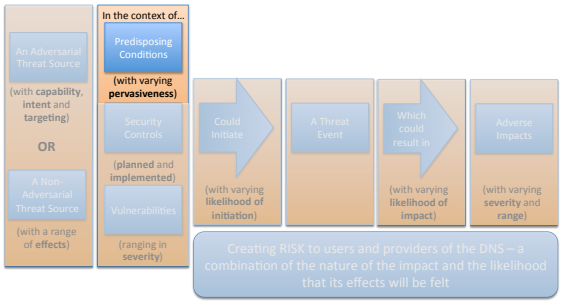
- Widespread infrastructure failure
- Key hardware failure
- Earthquakes
- Hurricanes
- Tsunami
- Blackout/Energy Failure
- Snowstorm/blizzard/ice-storm

Range of effect (to DNS providers) (Non-adversarial threat sources)

10 -- sweeping, involving almost all DNS providers
8 -- extensive, involving most DNS providers (80%?)
5 --wide-ranging, involving a significant portion of DNS providers (30%?)
3 --limited, involving some DNS providers
1 -- minimal, involving few if any DNS providers

Figure 14

"... in the context of: <u>Predisposing Conditions</u> (with varying pervasiveness) that can positively or negatively impact risk..."



Predisposing Conditions

Managerial

- Legal standing (and relative youth) of ICANN
- Multi-stakeholder, consensus-based decision-making model
- Managerial vs. operational vs. technical security skills/focus/ resources
- Definitions of responsibility, accountability, authority between DNS providers
- Security project and program management skills/capacity
- Common ("inheritable") vs. hybrid vs. organization/system-specific controls
- Mechanisms for providing (and receiving) risk assurances, and establishing trust-relationships, with external entities
- Contractual relationships between entities

Operational

- Diverse, distributed system architecture and deployment
- Emphasis on resiliency and redundancy
- Culture of collaboration built on personal trust relationships
- Diverse operational environments and approaches

Technical

- Requirement for public access to DNS information
- Requirements for scaling

Pervasiveness Of Predisposing Conditions That Negatively Impact Risk

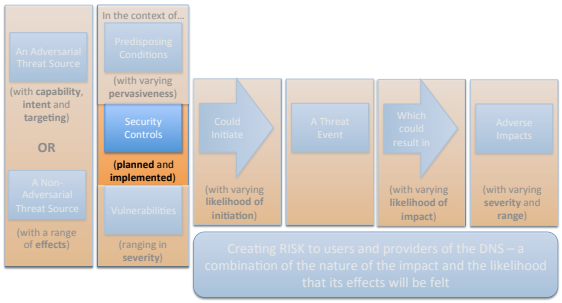
10 -- Very High -- Applies to all organizational missions/business functions
8 -- High -- Applies to most organizational missions/business functions
5 -- Moderate -- Applies to many organizational missions/ business functions
3 -- Low -- Applies to some organizational missions/business functions
1 -- Very Low -- Applies to few organizational missions/business functions

Pervasiveness Of Predisposing Conditions That Positively Impact Risk

.1 -- Very High -- Applies to all organizational missions/business functions
.3 -- High -- Applies to most organizational missions/business functions
.5 -- Moderate -- Applies to many organizational missions/ business functions
.8 -- Low -- Applies to some organizational missions/business functions
1 -- Very Low -- Applies to few organizational missions/business functions

Figure 15

"… Security Controls (both planned and implemented), and …"



Pervasiveness Of Controls
10 -- Controls are missing
8 -- Controls are acknowledged as needed
5 -- Controls are planned or being implemented
2 -- Controls are implemented
1 -- Controls are effective

Controls

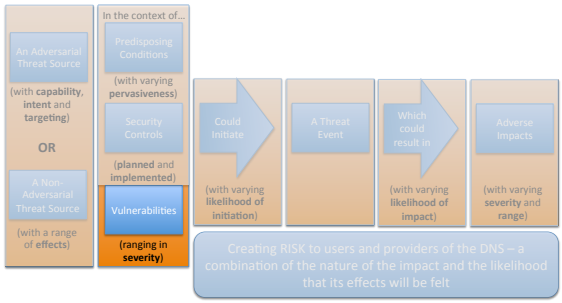
Management Controls
- Security Assessment and Authorization
- Planning
- Risk Assessment
- System and Services Acquisition
- Program Management

Operational Controls
- Awareness and Training
- Configuration Management
- Contingency Planning
- Incident Response
- Maintenance
- Media Protection
- Physical and Environmental Protection
- Personnel Security
- System and Information Integrity

Technical Controls
- Access Control
- Audit and Accountability
- Identification and Authentication
- System and Communications Protection

Figure 16

"…Vulnerabilities (which range in severity)…"



Vulnerability Severity

10 -- Very High -- Relevant security control or other remediation is not implemented and not planned; or no security measure can be identified to remediate the vulnerability.

8 -- High -- Relevant security control or other remediation is planned but not implemented.

5 -- Moderate -- Relevant security control or other remediation is partially implemented and somewhat effective.

2 -- Low -- Relevant security control or other remediation is fully implemented and somewhat effective.

1 -- Very Low -- Relevant security control or other remediation is fully implemented, assessed, and effective.

Vulnerabilities

Managerial
- Interventions from outside the process
- Poor inter-organizational communications
- External relationships/dependencies
- Inconsistent or incorrect decisions about relative priorities of core missions and business functions
- Lack of effective risk-management activities
- Vulnerabilities arising from missing or ineffective security controls
- Mission/business processes (e.g., poorly defined processes, or processes that are not risk-aware)
- Security architectures (e.g., poor architectural decisions resulting in lack of diversity or resiliency in organizational information systems)

Operational
- Infrastructure vulnerabilities
- Business continuity vulnerabilities
- Malicious or unintentional (erroneous) alteration of root or TLD DNS configuration information
- Inadequate training/awareness
- Inadequate incident-response

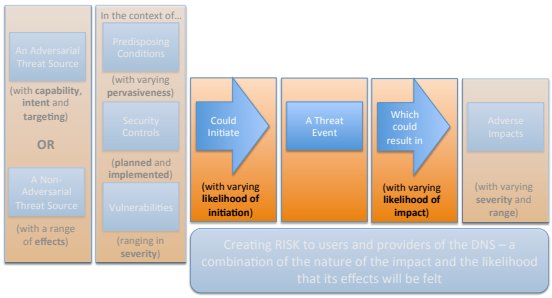
Technical (Under Discussion)
- IDN attacks (lookalike characters etc. for standard exploitation techniques)

Technical (System And Network)
- Recursive vs. authoritative nameserver attacks
- DDOS
- Email/spam

Technical (Identification And Authentication)
- Data poisoning (MITM, Cache)
- Name Chaining (RFC 3833)
- Betrayal by Trusted Server (RFC 3833)
- Authority or authentication compromise
- Packet Interception
- Man in the middle
- Eavesdropping combined with spoofed responses

Figure 17

"… could Initiate (with varying likelihood of initiation) a Threat Event which could result (with varying likelihood of impact)…"



Threat Events

Zone does not resolve or is not available
Zone is not correct or does not have integrity

Likelihood of initiation (by adversarial threat sources)

10 -- Very High -- Adversary is almost certain to initiate the threat-event
8 -- High -- Adversary is highly likely to initiate the threat event
5 -- Moderate -- Adversary is somewhat likely to initiate the threat event
2 -- Low -- Adversary is unlikely to initiate the threat event
0 -- Very Low -- Adversary is highly unlikely to initiate the threat event

Likelihood of initiation (by non-adversarial threat sources)

10 -- Very high -- Error, accident, or act of nature is almost certain to occur; or occurs more than 100 times a year.
8 -- High -- Error, accident, or act of nature is highly likely to occur; or occurs between 10-100 times a year.
5 -- Moderate -- Error, accident, or act of nature is somewhat likely to occur; or occurs between 1-10 times a year.
2 -- Low -- Error, accident, or act of nature is unlikely to occur; or occurs less than once a year, but more than once every 10 years.
0 -- Very Low -- Error, accident, or act of nature is highly unlikely to occur; or occurs less than once every 10 years.

DSSA default value

Likelihood of impact

10 -- Very High -- If the threat event is initiated or occurs, it is almost certain to have adverse impacts.
8 -- High -- If the threat event is initiated or occurs, it is highly likely to have adverse impacts.
5 -- Moderate -- If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
2 -- Low -- If the threat event is initiated or occurs, it is unlikely to have adverse impacts.
0 -- Very Low -- If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.

Figure 18

"… <u>Adverse Impacts</u> (with varying severity and range)."

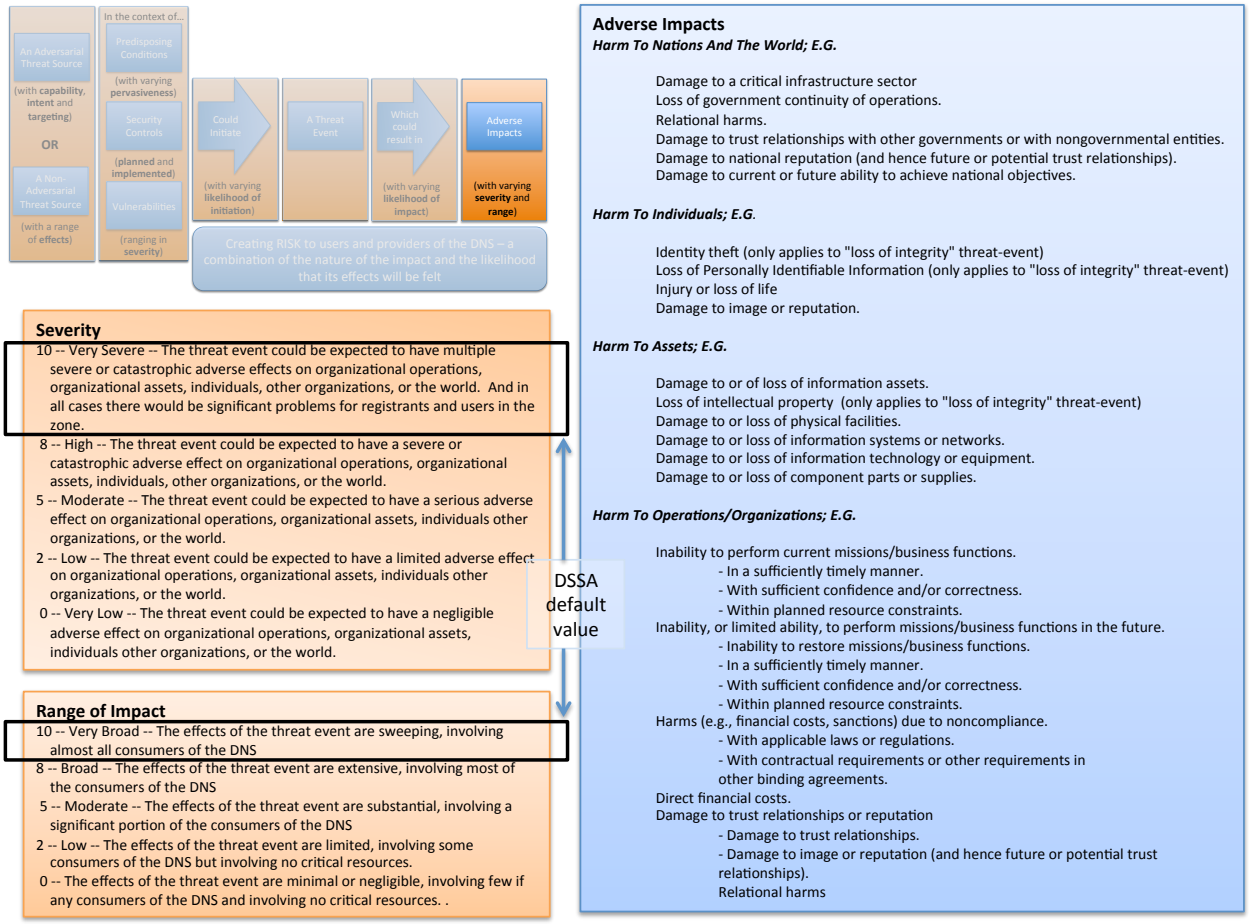


Figure 19

Larger versions of these charts are included in the Appendix.

This framework has also been recast as an Excel worksheet that is the data-collection tool that was "alpha tested" by the DSSA as it moved on to very-rapidly develop the broad risk-topics described in the Findings section above. The worksheet is extremely helpful in summarizing a very rich framework in an understandable way and in actually computing the numerical risk assessment value. It is available to the community on the DSSA wiki. Here is a link to the page where all of the risk scenario worksheets (templates and completed worksheets) are archived.

https://community.icann.org/display/AW/Risk+Scenario+worksheets

<u>Observations</u>

- The DSSA strongly encourages interested members of the community to explore the details of the risk-assessment framework by downloading the Excel worksheet and using this in

conjunction with the same information presented in the pictorial tables above and also contained in the Appendices to this report.

The DSSA intends to add several capabilities to the next generation of the worksheet:

- The worksheet will be broken up into several sections to make is easier to separate the "create a scenario" activity (which will likely be done by individuals working independently) from the "evaluate a scenario" job (which will be probably be done by groups of people)
- The next generation of the worksheet may separate the scales that are used to evaluate the current state of risk factors (such as vulnerabilities, controls, etc.) from those that evaluate the probability or likelihood of the events and impacts.

4.2.3. Protocol for handling confidential information

The DSSA-WG Charter recognized that sub-groups might need to access sensitive or proprietary information in order for the DSSA-WG to do its work. The DSSA needed to clearly describe the way it would handle that confidential information in order to assure information providers that information disclosure would always be under their control. The following diagram summarizes the protocol that the DSSA developed to address this. The details of the protocol are included in the Appendix.

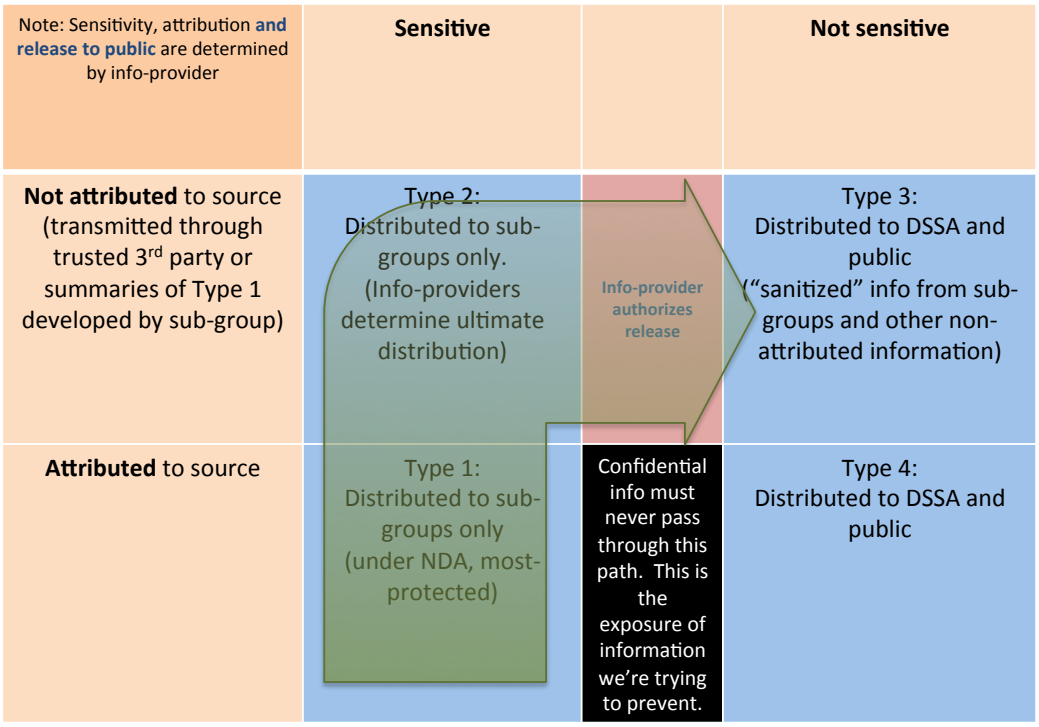


Figure 20

In the words of the protocol "The primary goal of these guidelines is to make sure that the people sharing highly sensitive information with sub-groups are assured that their information will not find its way out of those sub-groups without their permission."

In essence, information progresses through four types – "Type 1" which is the most sensitive information through "Type 4", which is the most widely distributed.

Observations

- It would be extremely helpful to future DSSA-like activities if these protocols (and the systems to support them) could be agreed to and in place prior to starting the analysis. It seems reasonable to presume that as the security-management capability of the ecosystem grows more mature, future working groups are likely to face similar requirements for handling sensitive information. Removing the need to reinvent these processes (and convince information providers that they're effective) will make those efforts much more productive.

- DSSA members are not in agreement as to whether confidential information is even required in order to complete their work. What is clear is that the DSSA has no authority to command DNS-providers to share sensitive details of their day to day security operations – the DSSA can only request such information, and thus any information that is volunteered must be handled with great care.

4.3. Tentative approach for the next ("go deep") phase

This section of the report describes the work that remains – what the DSSA is calling the "go deep" part of the work – where the methods and protocols that have been developed to date will be used to complete the work posed in the Charter.

While the narrative which follows (and the Appendices that support it) describe the work-steps that remain, the DSSA is continuing its habit of not specifying delivery dates. Most of the work that is planned has never been attempted before in the ICANN ecosystem and the working group prefers not to make promises until it is clear that they can be kept.

Observations

- The DSSA is chartered as a one-time working group effort – a project. It had a beginning and middle, and is approaching its end with the conclusion of this remaining work. However "risk-assessment" in the risk-management context is a function that, like any other ongoing organizational activity, should continue indefinitely.

- The DSSA hopes that its one-time effort can provide useful insights as the ICANN Board DNS Risk Management Framework Working Group (DNRMF WG) conducts its initial baseline assessment and moves toward its goal of establishing an ongoing risk-management framework and system for the DNS.

- If the DNRMF baseline assessment begins to overtake the DSSA, it is hoped that the two efforts can be coordinated in a way that reduces the workload on the all-volunteer DSSA team.

4.3.1. Approach

The diagram below depicts the remaining work in the context of the findings to date. The DSSA has identified five broad risk scenario topics that it plans to explore during the last phase of its work. The plan is to refine the tools that have been developed so far (by using them to explore one risk scenario topic) and then rolling them out to explore the remaining risk topics and engage ever-broader cross-sections of the community.

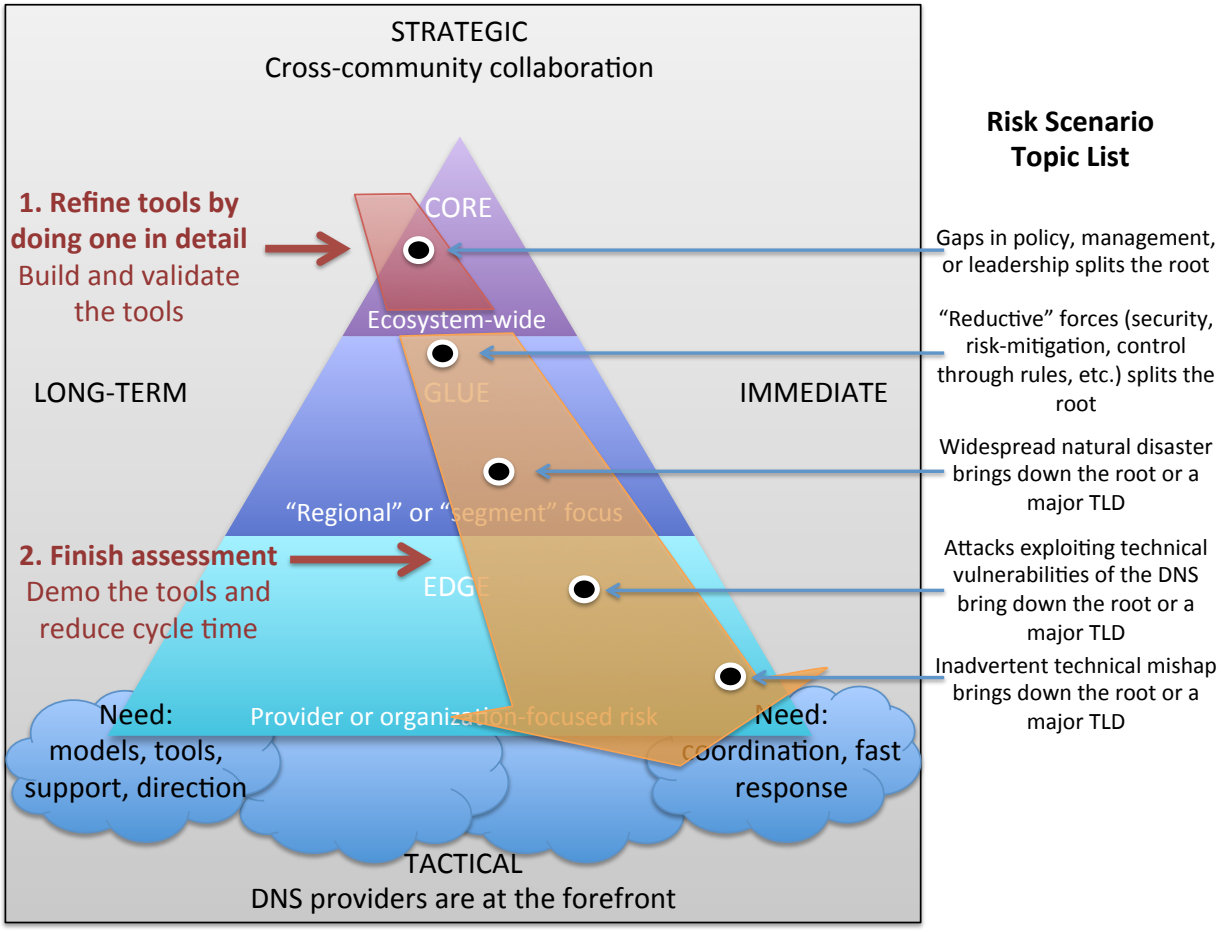


Figure 21

4.3.2. Work breakdown

The diagram that follows describes the current thinking of the working group as to how it will evaluate each risk-scenario topic.

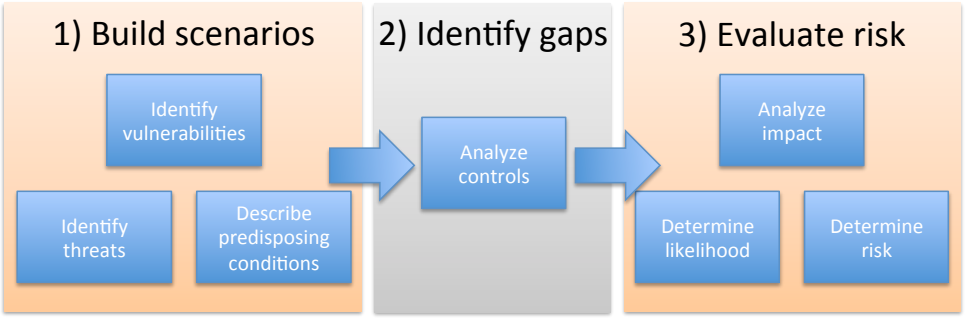


Figure 22

Step 1 – Build Scenarios

Individual working-group members use risk-scenario worksheets to quickly brainstorm a series of related scenarios based on the broad risk topic under discussion.

TASK 1-1: Identify the threat sources of concern

TASK 1-2: Identify potential threat-event scenarios, the relevance to the DNS, and the threat sources that could initiate the events

TASK 1-3: Identify vulnerabilities and predisposing conditions (which may increase or decrease risk) that affect the likelihood that threat events of concern result in adverse impacts to the organization

TASK 1-4: Develop consolidated scenarios and prepare scenario-evaluation surveys for the next step of the analysis

TASK 1-5: Evaluate the process with an eye to reducing cycle time and ease of use for subsequent efforts

Step 2 – Identify gaps

The working group uses a structured survey process to collectively evaluate each threat-scenario (threat-events, vulnerabilities and predisposing conditions) and then identify and evaluate gaps in security controls.

TASK 2-1: Characterize threat sources (capability, intent and targeting of adversarial threats, range of effect of non-adversarial threat sources) for each risk-scenario

TASK 2-2: Characterize vulnerabilities (by severity) and predisposing conditions (by pervasiveness) for each risk-scenario

TASK 2-3: Identify security controls that are the most relevant to addressing each risk-scenario

TASK 2-4: Characterize the current state of those security controls (by the degree to which they are implemented across the ecosystem) for each risk-scenario

TASK 2-5: Develop consolidated scenarios and prepare scenario-evaluation surveys for the next step of the analysis

TASK 2-6: Evaluate the process with an eye to reducing cycle time and ease of use for subsequent efforts

Step 3 – Evaluate risk

The working-group uses a structured survey process to collectively evaluate the risk of each threat-scenario

TASK 3-1: Assess the likelihood that each risk-scenario will be initiated, considering the characteristics of the threat sources that have been identified

TASK 3-2: Assess the likelihood that each risk-scenario will result in adverse impacts to the DNS, considering: the vulnerabilities and predisposing conditions identified; and ecosystem susceptibility reflecting security controls planned or implemented to impede such events

TASK 3-3: Determine the risk to the DNS from each risk-scenario considering the impact that would result from the events and the likelihood of the events occurring

TASK 3-4: Develop consolidated scenarios and publish overall risk-assessment

TASK 3-5: Evaluate the process with an eye to reducing cycle time and ease of use for subsequent efforts

Observations

- These steps and tasks will be repeated for each of the five broad risk-scenario topics that have been identified. The first iteration will (hopefully) be the slowest as methods are restructured and tested.
- One objective of the working group is to determine whether this risk-assessment methodology could be refined to the point that the whole process can be completed in as little as an hour. The thought is that by simplifying and shortening the process to that extent, it might also become a useful tool for a first-responder team within a DNS-provider that is facing a rapidly moving security situation.
- At a minimum, the DSSA hopes to refine these methods to the point that they will be an attractive way to promulgate best practices across the ecosystem, as well as providing a platform to quickly distribute updates based on emerging threats.

4.4. After DSSA Concludes – Ongoing Risk Assessment

The members of the DSSA hope that their work will contribute to an ongoing community wide effort to monitor the security and stability of the DNS. The working group will refine the results, methods and tools presented in this report with that goal in mind during the last phase of its work.

Here then are the final observations that the DSSA would like to share with the community in this report:

- The baseline assessment that the DSSA is delivering is just that – a momentary picture of the state of DNS security and stability that will probably be obsolete before it is published.
- The larger value of this effort is most likely to be found in the methods and tools that the DSSA has developed along the way to completing that assessment – methods and tools which the DSSA hopes will be applicable many times, by many members of the community.
- The DSSA notes that these tools have been developed so that they can be widely shared amongst the community, applied many times, by different organizations, in a repeatable way, and in a format that lends itself to rapid consolidation. The DSSA is hopeful that these reusable tools will find a broad audience and wide use.