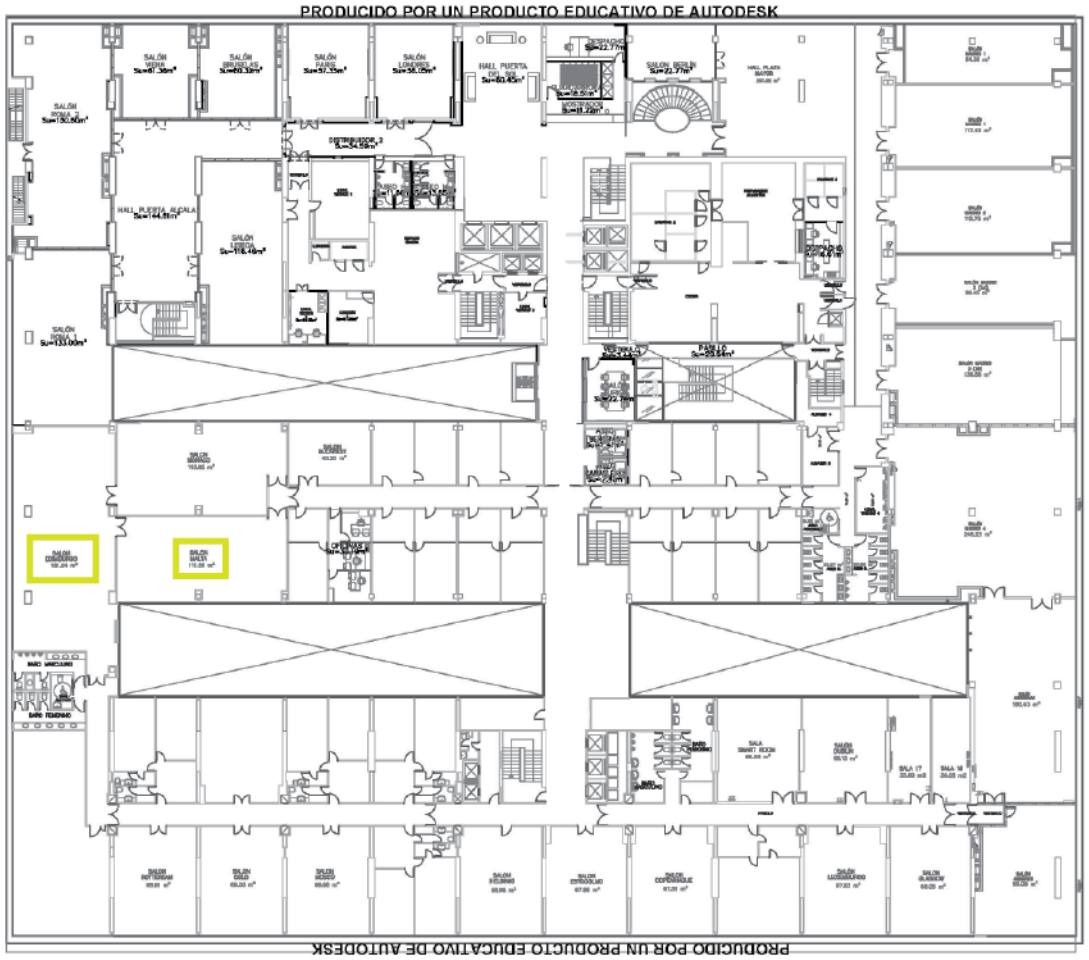
Second Security, Stability, and Resiliency Review (SSR2)

Plenary Meeting 11 | Madrid Face-to-Face
Day 1: 14 May 2017

Index

Meeting Logistics

- Observers may join in-room or online. Observers may input throughout.
- Restrooms:
  - Exit salon Edinburgo, restrooms immediately on your right
- Breaks (Salon Malta next door):
  - 10:30 – 10:40 coffee
  - 12:30 – 13:15 working lunch
  - 15:00 – 15:10 coffee



Agenda – Day One

1. 08:00 – 08:30
   Welcome, Rollcall, Statement of Interest Updates, Opening Remarks
2. 08:30 – 10:00
   Threat Landscape and DNS Symposium Follow-up – Briefing and Discussion
3. 10:00 – 12:30
   SSR1 Implementation Briefing: ICANN Office of the Chief Technology Officer (OCTO) Staff

10:30 – 10:40 Break

12:30 – 13:15 Review Team Lunch

4. 13:15 – 14:30
   SSR2-RT Reflection on SSR1 Implementation Briefings - Discussion
5. 14:30 – 15:30
   Identifier Technology Health Indicators (ITHI) & DNS Abuse Reporting (DART) Discussion

15:00 – 15:10 Break

6. 15:30 – 16:30
   AOB, Recap of Action Items
7. 16:30 – 17:00
   Review of Tomorrow's Agenda, Closing Remarks

ICANN Expected Standards of Behavior

Those who take part in ICANN's multistakeholder process, including Board, staff and all those involved in SO and AC councils, undertake to:

Act in accordance with ICANN's Bylaws. In particular, participants undertake to act within the mission of ICANN and in the spirit of the values contained in the Bylaws.

Adhere to ICANN's conflict of interest policies.

Treat all members of the ICANN community equally, irrespective of nationality, gender, racial or ethnic origin, religion or beliefs, disability, age or sexual orientation; members of the ICANN community should treat each other with civility both face-to-face and online.

Respect all members of the ICANN community equally and behave according to professional standards and demonstrate appropriate behavior. ICANN strives to create and maintain an environment in which people of many different backgrounds and cultures are treated with dignity, decency and respect. Specifically, participants in the ICANN process must not engage in any type of harassment. Generally, harassment is considered unwelcome hostile or intimidating behavior -- in particular, speech or behavior that is sexually aggressive or intimidates based on attributes such as race, gender, ethnicity, religion, age, color, national origin, ancestry, disability or medical condition, sexual orientation or gender identity.

Protect the organization's assets and ensure their efficient and effective use.

Act fairly and in good faith with other participants in the ICANN process.

Conduct themselves in accordance with ICANN policies.

Support the maintenance of robust mechanisms for public input, accountability, and transparency so as to ensure that policy development and decision-making processes will reflect the public interest and be accountable to all stakeholders.

Listen to the views of all stakeholders when considering policy issues. ICANN is a unique multistakeholder environment. Those who take part in the ICANN process must acknowledge the importance of all stakeholders and seek to understand their points of view.

Work to build consensus with other stakeholders in order to find solutions to the issues that fall within the areas of ICANN's responsibility. The ICANN model is based on a bottom-up, consensus-driven approach to policy development. Those who take part in the ICANN process must take responsibility for ensuring the success of the model by trying to build consensus with other participants.

Promote ethical and responsible behavior. Ethics and integrity are essential, and ICANN expects all stakeholders to behave in a responsible and principled way.

Facilitate transparency and openness when participating in policy development and decision-making processes.

Act in a reasonable, objective and informed manner when participating in policy development and decision-making processes. This includes regularly attending all scheduled meetings and exercising independent judgment based solely on what is in the overall best interest of Internet users and the stability and security of the Internet's system of unique identifiers, irrespective of personal interests and the interests of the entity to which individuals might owe their appointment.

Welcome
Rollcall
Statement of Interest Updates
Opening Remarks

ICANN

Threat Landscape & DNS Symposium Follow-Up

ICANN OCTO Staff

SSR1 Implementation Briefing

ICANN OCTO Staff

SSR1 Implementation Highlights

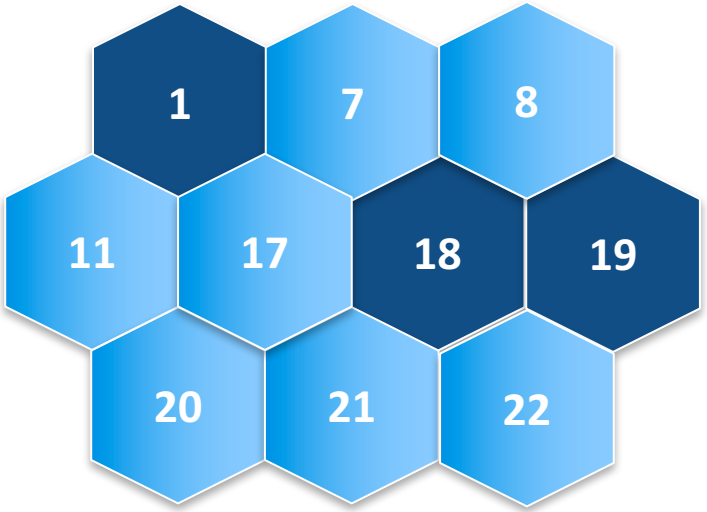
The ICANN organization has invested significant time and effort to implement all 28 recommendations from the first SSR Review Team, as approved by the ICANN Board in October 2012.

Highlights include:

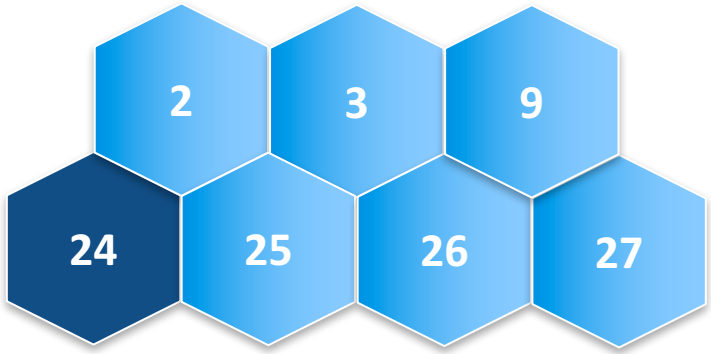
- The Office of Chief Technology Officer (OCTO) was announced in June 2014, with a mission that is directly aligned with the spirit of SSR1 recommendations. David Conrad took on the role in August 2014, and has since built a team of 14 professionals who work to understand and ensure the security, stability and resiliency of the unique identifier systems.
- The creation of OCTO helped align the mission of the Office of the CTO Security Stability and Resiliency team (OCTO SSR team) with the fast-paced technical advancements of the Internet.
- The SSR Framework was created as a result of defining ICANN's SSR remit and technical mission. The framework is now published annually.
- The ICANN organization has increased and improved its outreach and engagement efforts with SO/ACs to promote SSR-related best practices.

SSR1 Recommendations

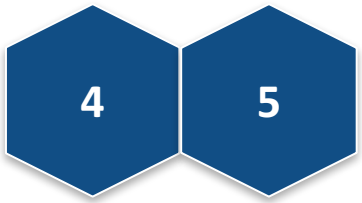
SSR Framework



ICANN's SSR Role & Remit Within It's Limited Mission

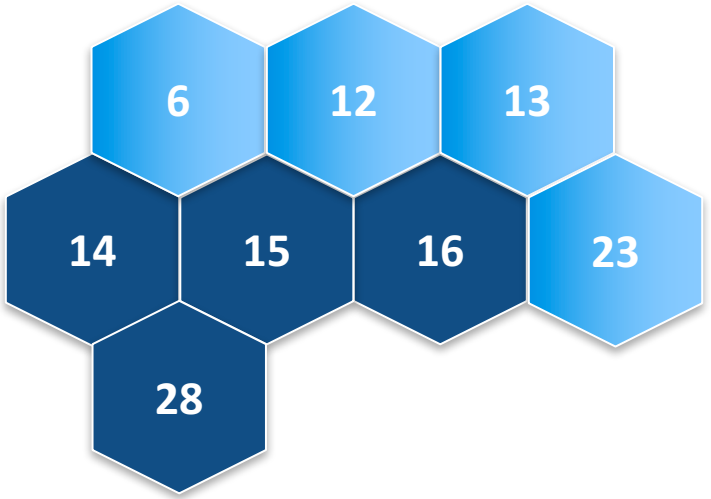


SSR Relationships to Support ICANN's Work



Compliance

SSR Community Outreach & Info Sharing – Security Threats & Mitigation



Core Recommendations

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.

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. **4**

ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal. **5**

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. **14**

15 ICANN should act as facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.

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.

18 ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework.

ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not harming ICANN's ability to operate effectively. The dashboard process being used to track implementation of the ATRT recommendations serves as a good model. **19**

24 ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.

ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information. **28**

SSR Framework

SSR1 Recommendation 1 – **Status and Deliverables**

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.

- Public comment was taken on a draft statement between May-Sept 2012; it was subsequently revised in Oct 2012.
- The updated statement was published on ICANN's website and incorporated in the FY 14 SSR Framework and is part of SSR SOP in which SSR Framework and statement is periodically reviewed and updated as needed (FY15-16 SSR Framework). This statement also has been incorporated into other ICANN documentation.

ICANN's Mission & Core Values

ICANN Bylaws, as amended 1 October 2016, state:

"The mission of the Internet Corporation for Assigned Names and Numbers ("**ICANN**") is to ensure the stable and secure operation of the Internet's unique identifier systems as described in this Section 1.1(a) (the "**Mission**")

Definitions For This Framework

Security – the capacity to protect Internet Identifier Systems and prevent misuse.

Stability – the capacity to ensure that Internet Identifier Systems operate as expected, and that users of these systems have confidence that the systems operate as expected or intended.

Resiliency – the capacity of Internet Identifier Systems to effectively withstand, tolerate, or survive malicious attacks and other disruptive events without interruption or cessation of service.

The Challenge

- Attacks against global network operations and misuse of Identifier Systems (especially the DNS)
  - DDoS attacks
  - Botnet attacks
  - BGP hijackings & service disruptions

- Trends observed:
  - Continued growth in adoption of DNSSEC by TLD operators and resolvers, as well as increasing DNSSEC adoption in delegated domain names
  - Expansion of root server instances worldwide
  - Delegation of new ccTLDs – both Internationalized Domain Name and non-IDN ccTLDs – in a growing number of languages and character sets
  - Launch of the new gTLD program in 2013, leading to delegation of hundreds of new gTLDs
  - Increased interest in cybersecurity capability building, stimulating the delivery of DNS training beyond operational communities to law enforcement and the legal community

ICANN's SSR Role & Remit

- Using a global multistakeholder approach, ICANN facilitates the security, stability and resiliency of the Internet's unique Identifier Systems through coordination and collaboration.

- Within its technical mission, ICANN's SSR role encompasses three categories of responsibilities:
  - ICANN's operational responsibilities (organizational risk management of internal operations including L-root, DNS operations, IANA functions (e.g. DNSSEC key signing operations), new gTLD operations, Time Zone Database Management);

  - ICANN's involvement as a coordinator, collaborator and facilitator with the global community in policy and technical matters related to the Internet's unique identifiers;

  - ICANN's engagement with others in the global Internet ecosystem.

ICANN's SSR-Related Activities

- A few examples of ICANN's activities supporting a secure, stable and resilient Unique Identifier ecosystem centers on the:
  - Support Operational Excellence in activities led by PTI, IT, DNS Ops, and Global Domains Division
  - Support ICANN's research team's Identifier Technologies Health Indicators development
  - Develop proof of concept data analytics for tracking, measuring, or reporting domain name and registration service misuse or abuse
  - Provide Technical Engagement (through subject matter expertise and thought leadership, community engagement, conducting Identifier Systems training and capability building activities where requested)
  - Develop "force multiplier" relationships with CERT or other stakeholders to expand the pool of experienced and qualified trainers of capability building programs created by the OCTO SSR Team
  - Encourage adoption and awareness of SSR best practices (e.g. DNSSEC) by enterprises, users and operators
  - More details can be found at: https://www.icann.org/en/system/files/files/ssr-framework-fy15-16-30sep16-en.pdf

Responsibilities That Lie Outside of ICANN's Role in SSR

Responsibilities that lie outside ICANN's role in SSR include:

- ICANN does not play a role in policing the Internet or operationally combatting criminal behavior;
- ICANN does not have a role in the use of the Internet related to cyber-espionage and cyber-war;
- ICANN does not have a role in determining what constitutes illicit conduct on the Internet.
- ICANN does not directly operate the majority of the core DNS infrastructure.

How Security, Stability, & Resiliency Fit into ICANN's Functional Areas

- Security, Stability, & Resiliency is:
  - A Core Value for ICANN
  - One of the Five Strategic Objectives identified by ICANN's Strategic Plan
  - An overall thematic area, cutting across the organization
  - An essential element in ICANN projects and activities

SSR1 Recommendation 18 – **Status and Deliverables**

ICANN should conduct an annual operational review of its progress in implementing the SSR Framework and include this assessment as a component of the following year's SSR Framework.

1. Implement SSR Framework and update annually
2. Publish previous status of SSR Review Team implementation
3. Reflect SSR Framework in the Strategic and Operating Plans and budgets, with the status/progress being reviewed and reported annually for public input prior to the issuance of the following-year's Ops Plan and budget
4. Integrate SSR objectives and goals into ICANN's Organizational (structural) reviews

- Implemented as part of the FY 13 & FY 14 SSR Frameworks and will be repeated annually.
- The previous status of SSR RT implementation was published in Appendix C of the ATRT2 Report
- Elements of the SSR Framework are reflected in the Strategic and Operating Plans and budgets, with the status/progress being reviewed and reported annually for public input prior to the issuance of the following-year's Ops Plan and budget. Information is posted here.
- SSR objectives and goals are integrated into ICANN's Organizational (structural) reviews, as appropriate; these are scheduled every five years.

Security, Stability, & Resiliency in the ICANN Strategic Plan

- In October 2014, ICANN published a new Strategic Plan for fiscal years 2016-2020.
- As illustrated below, the ICANN Strategic Plan identifies a healthy, stable, and resilient Unique Identifier ecosystem as one of five strategic objectives for the organization.

Figure 4 – ICANN's Strategic Objectives (2016-2020)

SSR-Related KPIs

Objective	Goal
1-Evolve and further globalize ICANN	1.2-Bring ICANN to the world by creating a balanced and proactive approach to regional engagement with stakeholders
	1.3-Evolve policy development and governance processes, structures and meetings to be more accountable, inclusive, efficient, effective and responsive
2-Support a healthy, stable and resilient unique identifier ecosystem	2.1-Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem
	2.2-Proactively plan for changes in the use of unique identifiers, and develop technology roadmaps to help guide ICANN activities
	2.3-Support the evolution of domain name marketplace to be robust, stable and trusted
3-Advance organizational, technological and operational excellence	3.1-Ensure ICANN's long-term financial accountability, stability and sustainability
4-Promote ICANN's role and multistakeholder approach	4.1-Empower engagement with the existing Internet governance ecosystem at national, regional and international levels
	4.4-Promote role clarity and establish mechanisms to increase trust within ecosystem rooted in the public interest
5-Develop and implement a global public interest framework bounded by ICANN's mission	5.2-Promote ethics, transparency and accountability across the ICANN community

SSR1 Recommendation 19 – **Status and Deliverables**

ICANN should establish a process that allows the Community to track the implementation of the SSR Framework. Information should be provided with enough clarity that the Community can track ICANN's execution of its SSR responsibilities, while not harming ICANN's ability to operate effectively. The dashboard process being used to track implementation of the ATRT recommendations serves as a good model.

1

Publish annual SSR Framework and track progress against activities committed to in the previous year's Framework

- The publication of the annual SSR Framework tracks progress against the activities committed to in the previous year's Framework. This tracking mechanism, along with ICANN's regular project management reporting, and operating plans and budgets, provide more details on SSR (see Recommendation 2 for more information) and are all part of ICANN's SOP.

ICANN's SSR Role & Remit Within Its Limited Mission

SSR1 Recommendation 24 – **Status and Deliverables**

ICANN must clearly define the charter, roles and responsibilities of the Chief Security Office Team.

1

Address range of internal and external SSR responsibilities with Identifier Systems Security, Stability & Resiliency (OCTO SSR) Team, CTO (and staff), and CIO (and staff); OCTO SSR team to focus on current externally focused OCTO SSR, the CIO and team to focus on current internally focused OCTO SSR and the CTO and team looking towards future OCTO SSR risks and opportunities

- The Office of the CTO (including OCTO SSR), and the Office of the CIO closely coordinate to address the range of ICANN's internal and external SSR responsibilities. The OCTO SSR team works on externally focused ICANN-related SSR issues, the CIO and team work on internally focused security issues, and the OCTO Research team looks towards future SSR risks and opportunities within ICANN's limited scope and remit.

OCTO SSR

- ICANN OCTO SSR is a distributed team, with global reach and expertise in technical and technology policy issues impacting the Internet's unique Identifier Systems.

- The OCTO SSR team has an internal and external role, working across the organization and community to support ICANN's mission of preserving and enhancing the operational stability, reliability and global interoperability of the Internet.

- The team serves as a bridge between DNS operators, the technical community, public safety community, the operational security community, and other stakeholder groups.

Vision & Mission of ICANN OCTO SSR

- ***Vision***: To be a trusted partner in multi-stakeholder, collaborative efforts to ensure the security, stability, and resiliency of the Internet's unique Identifier Systems.

- ***Mission***: To preserve the security, stability and resiliency of the Internet's system of unique identifiers that ICANN helps coordinate, to promote user confidence and trust in these systems, and to strengthen these systems through capability building among the communities ICANN serves.

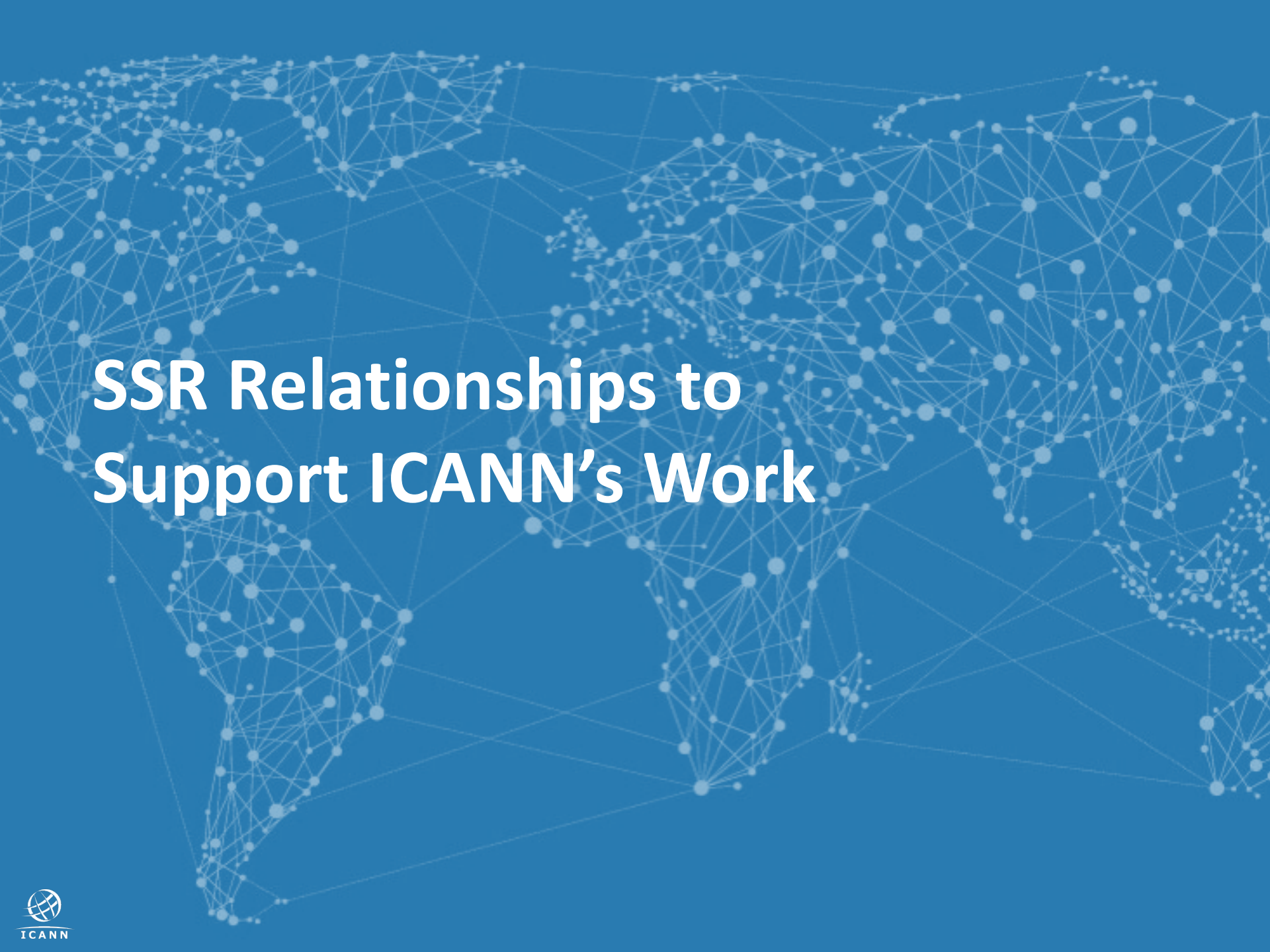
- The OCTO SSR Team contributes to achieving the overall mission of the Office of the CTO (OCTO):
  - To constantly improve knowledge about the identifiers ICANN helps coordinate;
  - To disseminate this information to the Internet community; and
  - To improve the technical operation of the Internet's system of unique identifiers in order to improve ICANN's technical stature.

- To do so, the OCTO SSR Team collaborates with OCTO Research Team, which is responsible for researching issues related to the Internet's system of unique identifiers, improving the security, stability, and resiliency of those identifiers, and providing internal and external Internet Technology Resources.

OCTO's Approach to Ensure a Secure, Stable, & Resilient Unique Identifier System

- Prevention through threat awareness and preparedness, collaboration and information sharing.
- Mitigation through information sharing and coordinated response
- Adoption of best practices through collaboration and capability building.
- Understanding through analysis of DNS data, domain registration service data and other data associated with identifier systems.
- Security awareness through competencies lending activities.
- Establishment of trustworthiness through transparency, communication and reliable execution.

SSR Relationships to Support ICANN's Work



SSR1 Recommendation 4 – **Status and Deliverables**

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.

1. Update OCTO SSR Team SOP work based on SSR activities
2. (Phase I) Post Memorandums of Understanding that indicate roles and responsibilities relevant to SSR
3. (Phase II) Provide additional detail on formal relationships ICANN has with key organizations
4. (Phase II) Extract and catalogue SSR-related elements of MOUs

- (Phase I) Many of ICANN's SSR relationships have been defined and publicized. As part of OCTO SSR Team SOP, this work will be updated periodically to keep pace with SSR activities. Memorandums of Understanding that indicate roles and responsibilities relevant to SSR have been signed with numerous entities; the list is posted here and will be updated as part of SOP, as needed.
- (Phase II) Extract and catalogue SSR-related elements of MOUs; Provide additional detail on formal relationships ICANN has with key organizations. This includes: 1) noting the "relationship," covering informal and formal arrangements; 2) documenting that some relationships are sensitive (not disclosed) and noting the industry best practices and conventions that are used to address this lack of disclosure.
- ICANN Security Awareness Resource Locator Developed - All stakeholders should learn how to protect themselves, their families, or their organizations against online threats. The resources on this page can help consumers, business or IT professionals avoid online threats or harm and make informed choices regarding (personal) data disclosure or protection.
- The document tracking ICANN SSR related roles and responsibilities has been completed and posted at https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf

Relationships in SSR

- ICANN maintains relationships with contracted parties (domain name registries and registrars, escrow providers and others), and partnerships, memoranda of understanding (MOU), accountability frameworks or exchange of letters.

- Other relationships may be less formal or unstructured, between ICANN and other international organizations or stakeholders in the ecosystem.

- ICANN's major agreements and related reports are published at: https://www.icann.org/en/about/agreements

- Detailed breakdown of ICANN's SSR Relationships is located at: https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf

- ICANN's Security Awareness Resource Locator page can be found at: https://www.icann.org/resources/pages/security-awareness-resource-2014-12-04-en

SSR1 Recommendation 5 – **Status and Deliverables**

ICANN should use the definition of its SSR relationships to maintain effective working arrangements and to demonstrate how these relationships are utilized to achieve each SSR goal.

1 (Phase I) Report on ICANN's progress toward SSR-related KSFs and KPIs involving SSR relationships

2 (Phase II) Include information on how key relationships noted in Recommendation 4 are used to achieve SSR goals (as part of SOP) in next SSR Framework/report on SSR activities

- (Phase I) Reporting on ICANN's progress toward SSR-related KSFs and KPIs involving SSR relationships is SOP, and can be found in ICANN's regular project management reporting, operating plans, SSR Framework, and SSR quarterly reports.
- (Phase II) Next SSR Framework/report on SSR activities will include information on how key relationships noted in Recommendation 4 are used to achieve SSR goals (as part of SOP).
- The document tracking ICANN SSR related roles and responsibilities has been completed and posted at https://www.icann.org/en/system/files/files/ssr-relationships-fy17-23jan17-en.pdf

SSR-Related KPIs

Objective	Goal
1-Evolve and further globalize ICANN	1.2-Bring ICANN to the world by creating a balanced and proactive approach to regional engagement with stakeholders
	1.3-Evolve policy development and governance processes, structures and meetings to be more accountable, inclusive, efficient, effective and responsive
2-Support a healthy, stable and resilient unique identifier ecosystem	2.1-Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem
	2.2-Proactively plan for changes in the use of unique identifiers, and develop technology roadmaps to help guide ICANN activities
	2.3-Support the evolution of domain name marketplace to be robust, stable and trusted
3-Advance organizational, technological and operational excellence	3.1-Ensure ICANN's long-term financial accountability, stability and sustainability
4-Promote ICANN's role and multistakeholder approach	4.1-Empower engagement with the existing Internet governance ecosystem at national, regional and international levels
	4.4-Promote role clarity and establish mechanisms to increase trust within ecosystem rooted in the public interest
5-Develop and implement a global public interest framework bounded by ICANN's mission	5.2-Promote ethics, transparency and accountability across the ICANN community

SSR Community Outreach & Information Sharing – Security Threats & Mitigation

ICANN

SSR1 Recommendation 14 – **Status and Deliverables**

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.

1

Outreach activities have been expanded and are reviewed annually as part of SOP (Standard Operating Procedure). The Security team provides both a service function to ICANN's Global Stakeholder Engagement team as subject matter experts, and a community function in outreach and engagement in SSR matters. A new Engagement Interface allows the community to see upcoming SSR and related outreach and engagement activities. This is an on-going obligation.

Security Criteria for Outreach & Engagement

Types of Events	Examples
ICANN Public Meetings	ICANN Los Angeles, Singapore, Buenos Aires, Dublin, Marrakech
ICANN Internal Meetings	Executive Meeting, IS-SSR Team, Board Workshop, Staff Training, Budget, Other
Meetings relevant to operational aspects of ICANN/IANA/L-root/DNSSEC, etc	IETF, DNS-OARC, RIPE NCC, NOGs, SSAC, RSSAC, LACNIC, LACTLD, BlackHat, InterOp, RSA, others
Meetings where ICANN collaborates on global threats/mitigation	APWG, MAAWG, cyber exercises, OAS, INTERPOL Global Cybercrime Expert Group (IGCEG), Europol, US FBI InfraGuard, APT-CST, APAC-FCACP, OSCE
Technical Engagement – Trainings & Capability Building	Attack & Contingency Response training (ACRP), Secure Registry Ops, DNSSEC, Law Enforcement & Govt, Commonwealth Cybercrime Initiative, Stop. Think.Connect Program, Secure The Human Project, ICANN Train-the-Trainers Program
Symposia, Invited SME conferences, continuing education	South School on Internet Governance, Dominios Latinoamerica, Security Analysts Summit Latin America, Mesa de Gobernanza de Internet
Engagement in Ecosystem, Multistakeholder model	IGF & regional IGFs, regional and national CERTs, European Commission, Organization for the Security and Cooperation in Europe, OECD

Engagement Criteria

Engagement Criteria		✓
Does the event support ICANN's SSR strategic objective?	1. Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem 2. Proactively plan for changes in the use of unique identifiers and develop technology roadmaps to help guide ICANN activities 3. Support the evolution of domain name marketplace to be robust, stable and trusted	
Does the event fit within one of the following functional areas:	1. Threat Awareness and Response 2. Identifier SSR Analytics 3. Trust-based Collaboration 4. Capability Building	
Is the event in support of a partnership, MOU or stakeholder relationship?		

Events & Activities Supported by ICANN OCTO SSR

As part of ICANN's matrix structure, the OCTO SSR team provides support to ICANN's Global Stakeholder Engagement (GSE) team, and other teams across the organization. Examples of the types of events and activities supported by the ICANN OCTO SSR team appear below:

- IETF Meetings
- CIS Registries Meeting in Budva, Montenegro
- DNS training with the National Crime Agency and Office of Fair Trading in London, UK
- DNS abuse training to police cybercrime units in Chile, Peru, Costa Rica, Colombia and Argentina
- DNSSEC training in various events worldwide
- DNS capability building training with LACTLD in St. Maarten & Paraguay
- MENOG in Dubai
- LACNIC/LACNOG in Uruguay and Colombia
- DNS training with Europol
- MAAWG, APWG, RIPE NCC and DNS-OARC
- OAS CICTE & World Economic Forum on Principles for Cyber Resilience
- APNIC, APTLD & APRICOT
- Providing talks via remote presentation, such as Georgetown University's Center for Intercultural Education and Development Cyber Security Program, OAS/CITEL, LACRALO, and the Universidad de los Andes
- Trainings at ICANN meetings (e.g. "How It Works", etc.)

SSR1 Recommendation 15 – **Status and Deliverables**

ICANN should act as facilitator in the responsible disclosure and dissemination of DNS security threats and mitigation techniques.

1 Publish Coordinated Vulnerability Disclosure document

2 Collaborate with operators and trusted security community entities on DNS security threats and mitigation techniques

- ICANN published a Coordinated Vulnerability Disclosure document in 2013. While the framework and SOP is in place, staff notes that because facilitation of responsible disclosure is an on-going obligation the work in this area is ongoing.
- Staff collaborates with operators and trusted security community entities on DNS security threats and mitigation techniques. This is related to Recommendation 28.
- The Identifier System Attack Mitigation Methodology report can be found at: https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf

Coordinated Vulnerability Disclosure Reporting at ICANN

- Coordinated Vulnerability Disclosure refers to a reporting methodology where a party (“reporter”) privately discloses information relating to a discovered vulnerability to a product vendor or service provider (“affected party”) and allows the affected party time to investigate the claim, and identify and test a remedy or recourse before coordinating the release of a public disclosure of the vulnerability with the reporter.

- Reporting Process: ICANN as affected party

- Reporting Process: ICANN as reporter

- ICANN as a vulnerability coordinator

Identifier System Attack Mitigation Methodology

- Community driven activity
- Mitigation methodologies for prioritized set of attacks
  - e.g., DDoS and BGP hijacking
  - Production of tech notes
- Tracking the evolution of the threat landscape and developing new mitigation methodologies
- The Identifier System Attack Mitigation Methodology report can be found at: https://www.icann.org/en/system/files/files/identifier-system-attack-mitigation-methodology-13feb17-en.pdf

SSR1 Recommendation 28 – **Status and Deliverables**

ICANN should continue to actively engage in threat detection and mitigation, and participate in efforts to distribute threat and incident information.

1 Identifier Systems SSR Activities Reporting

2 Coordinated Vulnerability Disclosure Reporting

- Identifier Systems SSR Activities Reporting
  - As part of our continuing commitment to transparency and accountability, the Identifier Systems SSR department publishes an activities report. The report describes the activities ICANN performs to maintain the security, stability, and resiliency of the Internet's global identifier systems. These activities include collaboration with ICANN, security and operations, and public safety communities, where our staff serves several roles.
  - The 1H 2015 activities report highlights ICANNs collaboration and stakeholder activities from January 1 through June 15, 2014. It summarizes activities performed as part of the identifier system SSR threat awareness and preparedness remit. It also provides progress reports on analytics or productivity improvement projects as well.
- Coordinated Vulnerability Disclosure Reporting at ICANN
- Posted the following Blogs:
  - Threats, Vulnerabilities and Exploits – oh my! 10 August 2015
  - What is ICANN IIS-SSR? 4 August 2015
  - Is This a Hack or an Attack? 15 September 2015
  - Top Level Domain Incident Response Resource Now Available 28 September 2015

OCTO SSR Activities Reporting

- Activities reports describe the activities OCTO SSR performs to maintain the security, stability, and resiliency of the Internet's global identifier systems.
- These activities include collaboration with ICANN, security and operations, and public safety communities, where ICANN organization staff serves several roles.
- Depending on the engagement or request, ICANN organization staff:
  - Offers security or Identifier System subject matter expertise,
  - Facilitates cooperative action among ICANN and other communities to maintain Identifier System SSR,
  - Conducts research, or
  - Supports the daily efforts of security or operations communities to mitigate the misuse or harmful use of the Identifier System or domain name registration services.
- These reports summarize activities OCTO SSR perform as part of their identifier system SSR threat awareness and preparedness remit
- The reports can be found at: https://www.icann.org/news/blog/identifier-systems-ssr-activities-reporting-834ea389-0f61-41d1-809e-b7a458633b87

SSR1 Recommendation 16 – **Status and Deliverables**

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.

1 Expand Outreach activities and processes to solicit input on the SSR Framework

2 Include SSR best practices and SSR topics in several Regional Engagement Strategies

3 Support a variety of capability-building initiatives by the Security Team

- Outreach activities and processes solicit input on the SSR Framework have been expanded and are part of ICANN's SSR SOP; activities are ongoing and are reviewed annually. For example: the Security team's ongoing work with security communities including the Anti Phishing Working (APWG), the Messaging, Malware and the Mobile Anti-Abuse Working Group (MAAWG) has resulted in participation by members of those communities in SSAC; through engagement with the International Criminal Law Network (ICLN) and Commonwealth Cybercrime Initiative (CCI), the Security team emphasizes the value of multistakeholder approaches to cybersecurity issues.
- Several Regional Engagement Strategies include SSR best practices and SSR topics are addressed by ICANN across all global regions.
- This is related to Recommendations 4, 5 and 14.
- At the request of stakeholders, the OCTO SSR team supports a variety of capability-building initiatives, such as DNSSEC training, ccTLD attack and contingency response training, law enforcement training, outreach at Network Operator Group meetings such as Caribbean Network Operators Group (CaribNOG), Middle East Network Operators Group (MENOG), among others.

OCTO SSR DNS Training

A key part of the technical engagement provided by the OCTO SSR team is in DNS training in response to community requests. The team has developed a curriculum, which includes modules on:

- DNS Basics (including an overview of participating in ICANN)
- Attack and Contingency Response Program for TLD operators
- DNS training for law enforcement and the operational security community
- DNSSEC training
- Secure Registry Operations course
- Identifier Systems Fundamentals for government or ministerial level stakeholders

Additional Outreach & Training

- ICANN regularly partners with the Network Startup Resource Center (http://nsrc.org/), based at the University of Oregon, to provide technical engagement with regional TLD organizations, universities and operators worldwide.

- ICANN also partners with country code top level domains organizations such as AfTLD, APTLD, LACTLD in this training.

International Developments

The OCTO SSR Team engaged in significant international activity during FY 15-16. Some examples are as follows:

- Capacity Building
- “Train the Trainers” Program
- DNSSEC Zone Signing by ccTLDs
- Strengthening Relationships with Public Safety Communities
- Threat Intelligence Reporting
- Reinforcing ICANN Community Relationships
- Program for GSE/OCTO SSR Engagement Tracking
- Remote Training
- Security and Technology Awareness Raising Activities

Additional information

Additional Information

Security Stability and Resiliency Review (SSR1)

SSR1 Implementation Quarterly Reports

SSR2-RT information

SSR Framework

ICANN Planning Process

ICANN Operating Plan 2016 – 2020

ICANN Strategic Plan

List of Presenters

Presenters	
Negar Farzinnia	Sr. Manager - MSSI
Karen Mulberry	Director - MSSI
David Conrad	Chief Technology Officer
John Crain	Chief Security, Stability & Resiliency Office
Steve Conte	Office of the CTO Programs Director
Dave Piscitello	VP of Security and ICT Coordinator
Patrick Jones	Sr. Director, Global Stakeholder Engagement

Reflection on SSR1 Implementation Briefings

SSR2-RT

SSR2-RT Reflection on SSR1 Implementation Briefings

- What are team members' thoughts on implementation?
- How can the RT best evaluate the implementation of recommendations?
- Do the recommendations of SSR1 effectively address all the concerns raised in the report?
- What additional information does the RT need to assess the effectiveness of its implementation?
- Next steps?

Identifier Technology Health Indicators (ITHI) & DNS Abuse Reporting (DART) Discussion

Alain Durand & Dave Piscitello

What is **ITHI**? Why Should You be Interested?

ITHI, or Identifier Technologies Health Indicators is a new ICANN initiative to "**measure**" the "**health**" of the "**identifiers**" that "**ICANN helps coordinate**".

The goal is to produce a set of indicators that will be **measured and tracked over time** that will help determine if the set of identifiers is overall doing better or worse.

This is a long term project, expected to run for many years. We are at the beginning, and it is important to get the community involved in the definition phase of the project.

What is the Scope of **ITHI**?

The scope of ITHI is all the unique Identifiers ICANN helps coordinate. It includes:

- DNS names
- IP addresses

This presentation will focus on the name track. The NRO has demanded to be in charge of the number track.

At some point, both tracks will be converged.

ICANN Strategic Plan 2016-2020

https://www.icann.org/en/system/files/files/strategic-plan-2016-2020-10oct14-en.pdf

2.1 Foster and coordinate a healthy, secure, stable, and resilient identifier ecosystem.

KEY SUCCESS FACTORS (OUTCOMES)

- Increased collaboration with the global community that improves the security, stability and resiliency of the unique identifier ecosystem (including updates of the root zone, Internet numbers registries, and protocol parameter registries, operation of the "L" root server, and other operational infrastructure supporting the identifier ecosystem).
- Ecosystem is able to withstand attacks or other events without loss of confidence in the operation of the unique identifier system.
- Unquestionable, globally recognized legitimacy as coordinator of unique identifiers.
- Reduction of government/industry/other stakeholders' concerns regarding availability of IP addresses.
- …

ITHI Project Timeline

http://www.icann.org/ithi
Mailing list: ithi@icann.org

March 2016: ITHI kick-off at ICANN55

Number community, through the NRO, joined the ITHI project but demanded to drive their own component.

September 2016: ITHI workshop at ICANN DC office
October 2016: ITHI workshop with M3AAWG, Paris
November 2016: ITHI session at ICANN57
January 2017: ITHI 1st public comment period closed

ITHI: Methodology

1) **Define Health**
2) Define Metrics to measure health
3) Get data to compute above metrics

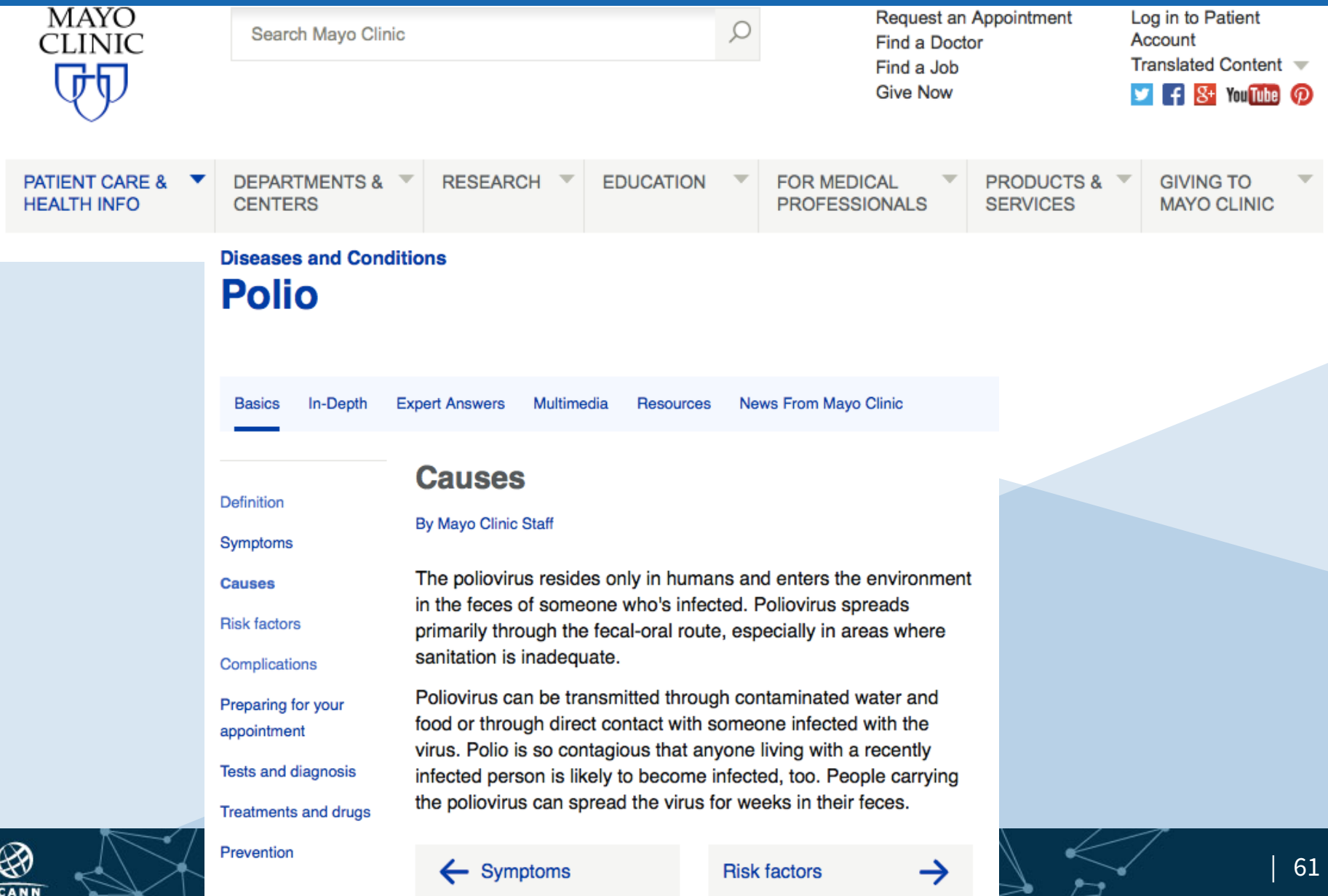
Status: - We are at step 1: defining health.
- We want to go to step 2, defining metrics from the above definitions

Heath: Definition

health |helTH|
noun
the state of being free from illness or injury
- Merriam Webster Dictionary

In the context of ITHI, we will look at "**health**" through the prism of known "**Problem Areas**" that we will try to measure.

Describing Diseases: the Mayo Clinic Example



Definition of Terms

Definition	A statement of the exact meaning of a word
Symptoms	A sign of the existence of something, especially of an undesirable situation
Causes	A person or thing that gives rise to an action, phenomenon, or condition
Risk Factors	A risk factor is any attribute, characteristic or exposure that increases the likelihood of developing a disease or injury.
Complications	A secondary disease or condition aggravating an already existing one
Impact	The effect or influence of one person, thing, or action, on another
Potential Treatment	Treatment: medical care given to a patient for an illness or injury

5 Problem Areas

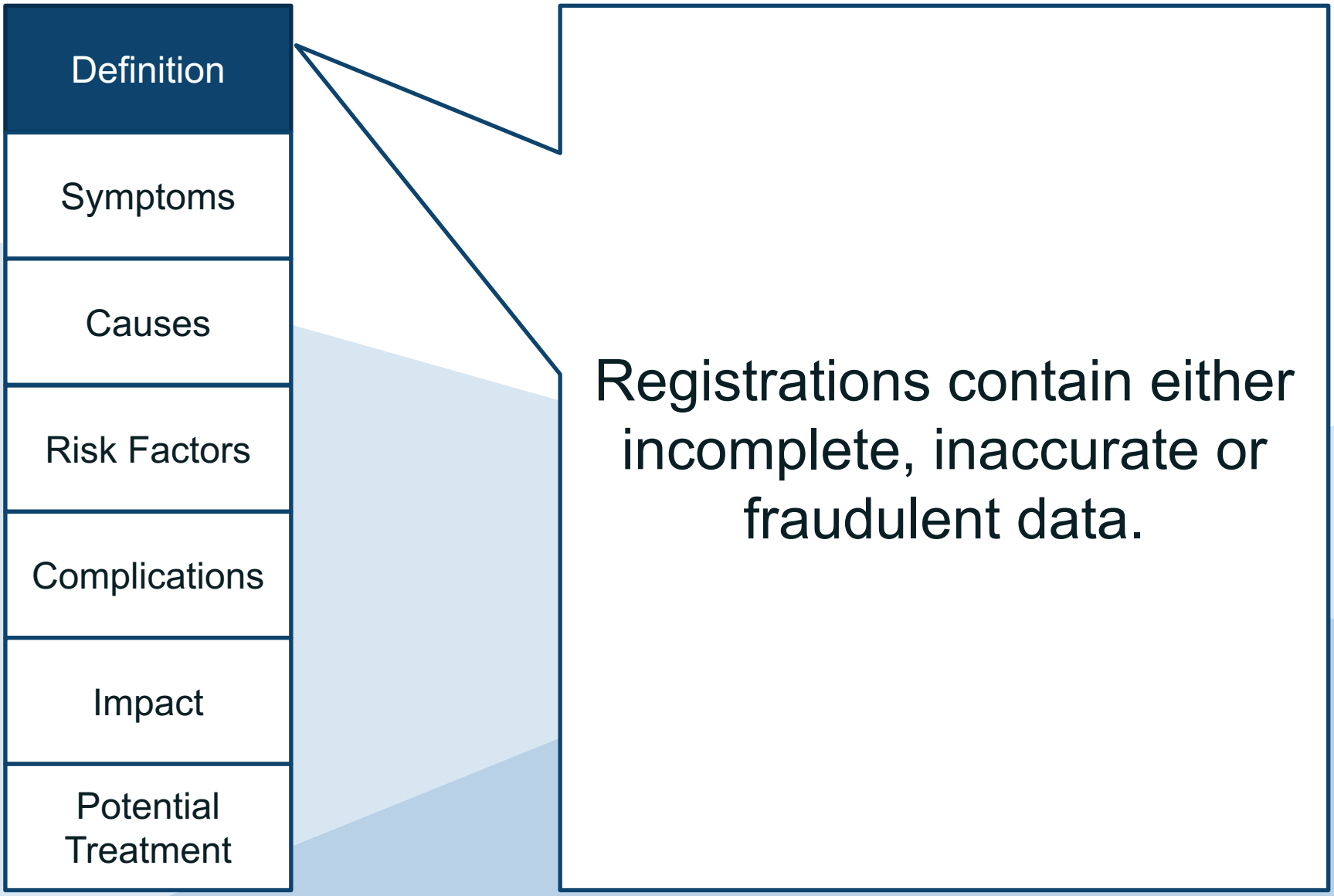
In the first phase of the name track of ITHI, we will focus on **5 problem areas**:

- ❑ Bad Data
- ❑ Abuse
- ❑ Excessive Traffic
- ❑ Leakage
- ❑ Lies

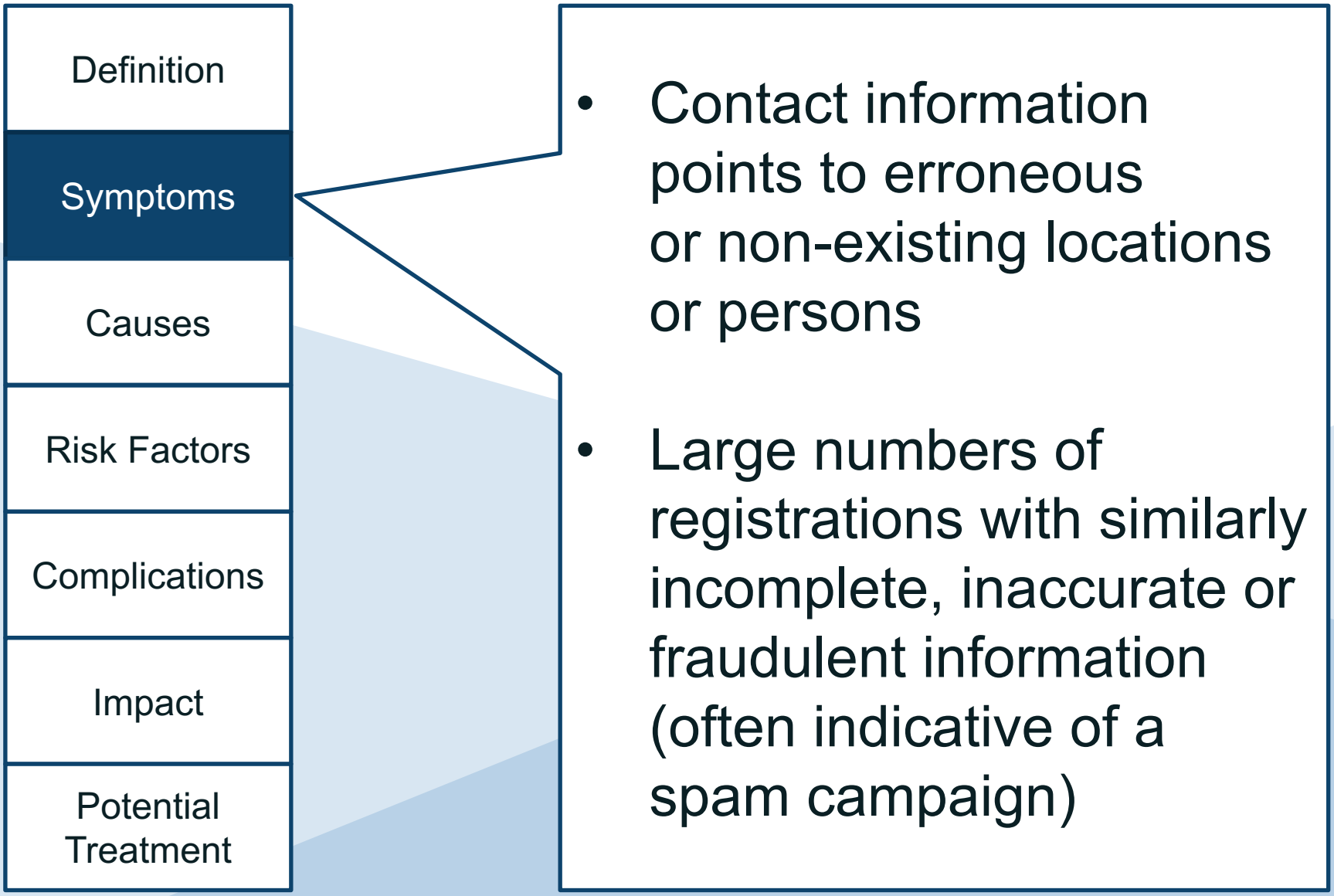
Over time, new problem areas could be defined, and/or some could removed.

Bad Data

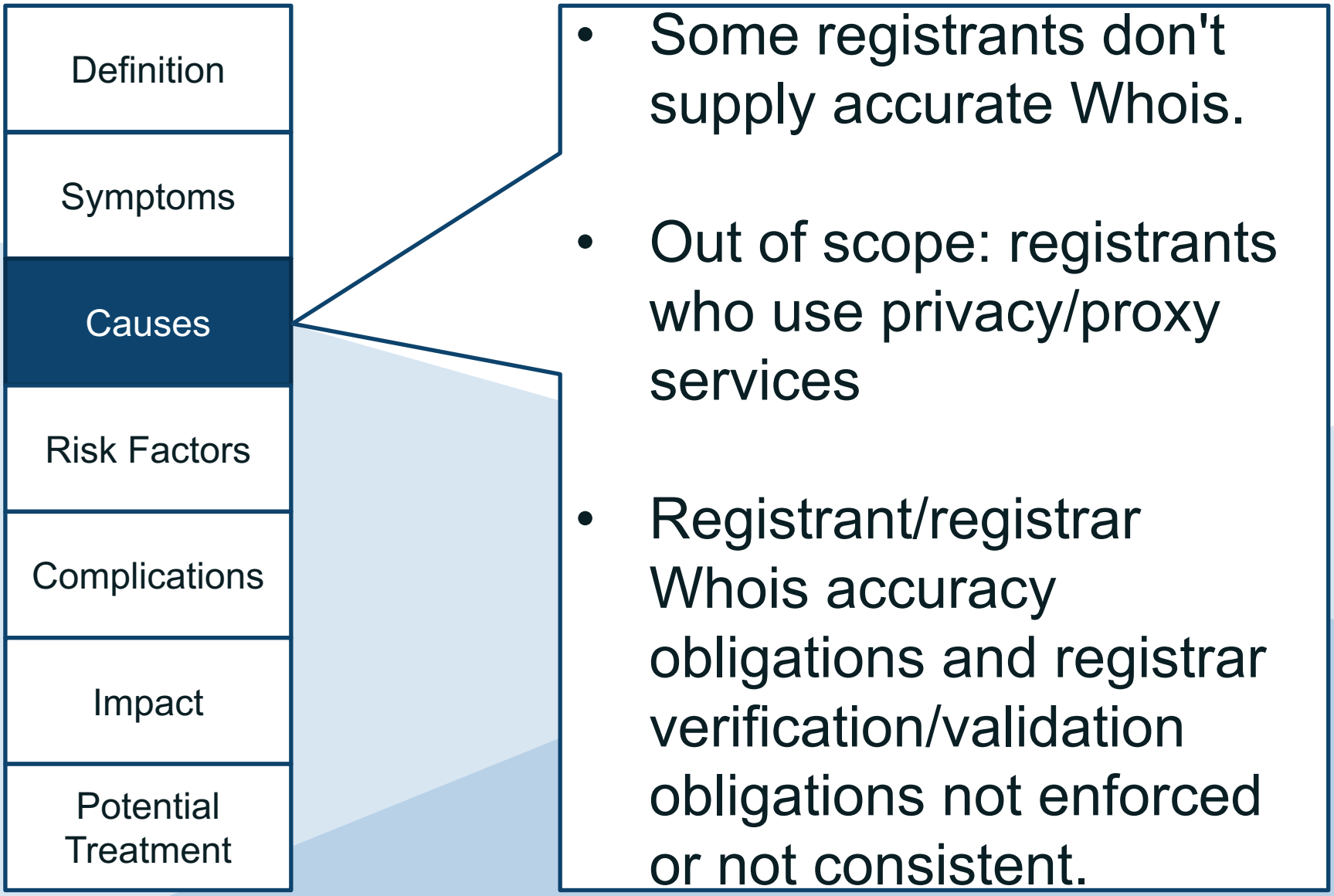
Bad Data


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
Registrations contain either incomplete, inaccurate or fraudulent data.

Bad Data


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Contact information points to erroneous or non-existing locations or persons
• Large numbers of registrations with similarly incomplete, inaccurate or fraudulent information (often indicative of a spam campaign)

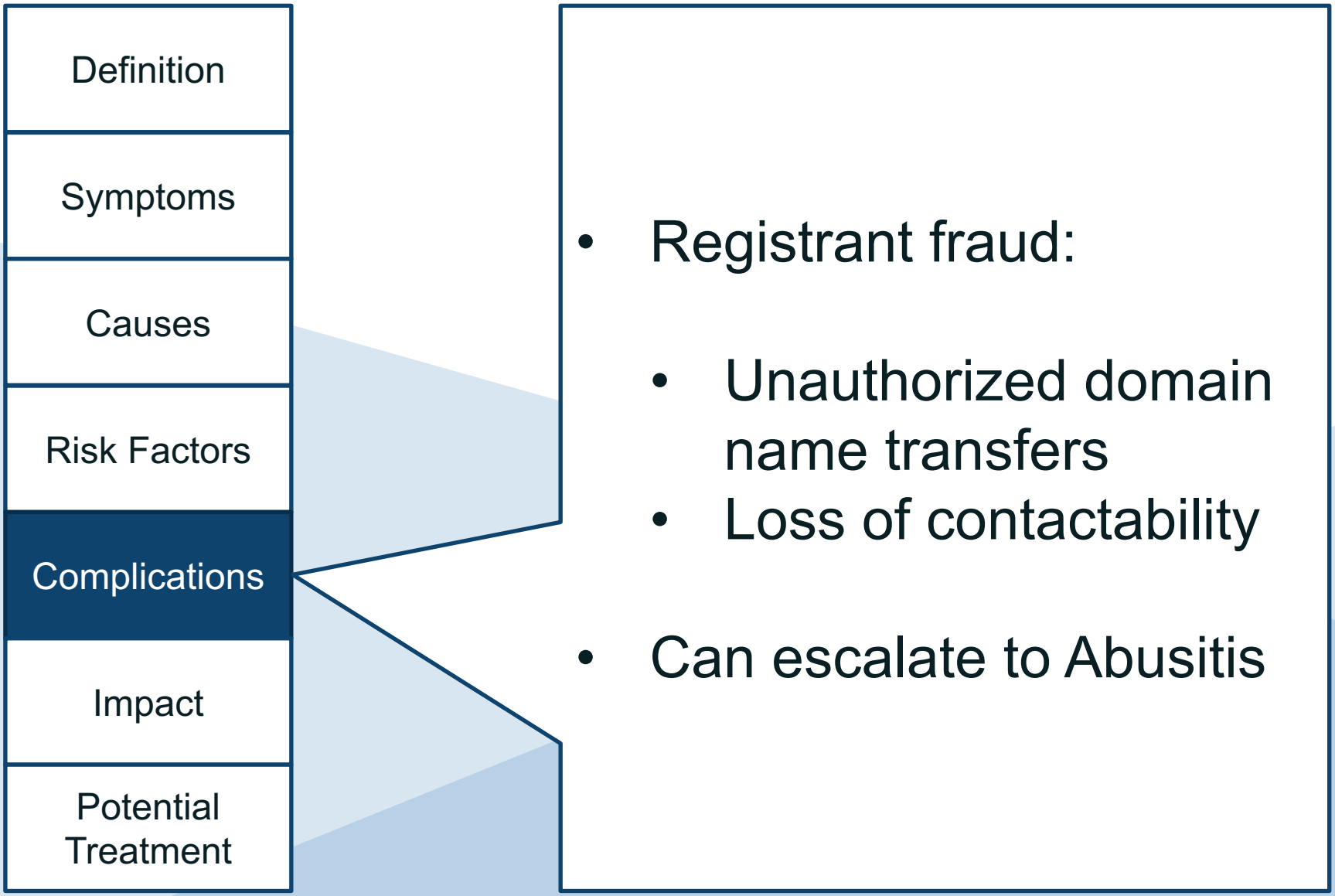
Bad Data


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Some registrants don't supply accurate Whois.
• Out of scope: registrants who use privacy/proxy services
• Registrant/registrar Whois accuracy obligations and registrar verification/validation obligations not enforced or not consistent.

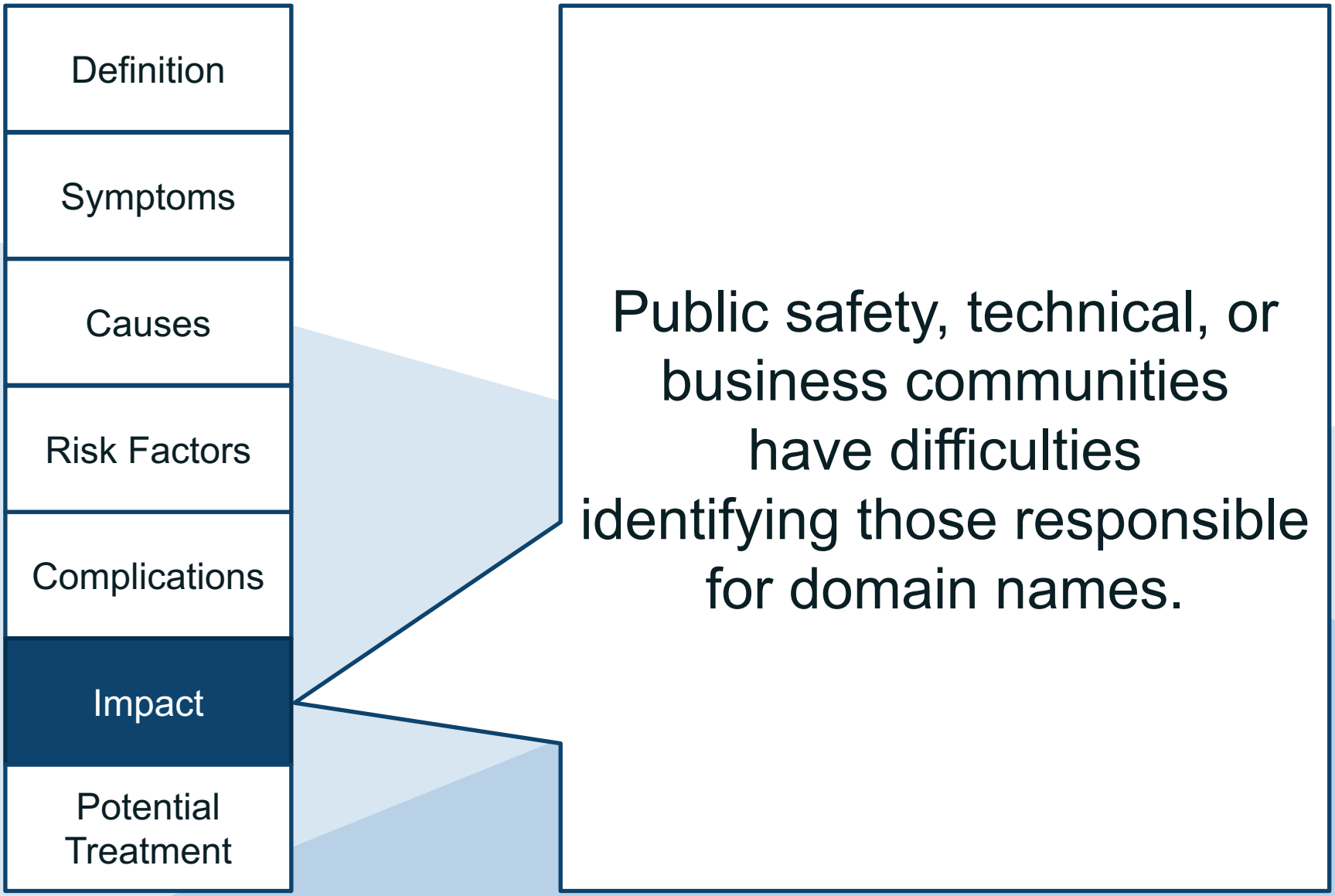
Bad Data

- Lack of agreed upon definition of accuracy
- Data accuracy/verification/validation is not enforced (or not enforceable) or not consistent
- National laws may be in conflict with getting access to accurate data (conflict of interest between accuracy and privacy)
- Data may exist but not accessible.

Bad Data


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Registrant fraud:
• Unauthorized domain name transfers
• Loss of contactability
• Can escalate to Abusitis

Bad Data


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
Public safety, technical, or business communities have difficulties identifying those responsible for domain names.

Bad Data

- Contract enforcement: RAA/Registration Agreements, Terms & Conditions
- Acceptable Use Policies that prohibit abuse and misuse of domain names
- National laws may force data accuracy checks

Abuse

Abuse

- **Definition**
- Symptoms
- Causes
- Risk Factors
- Complications
- Impact
- Potential Treatment

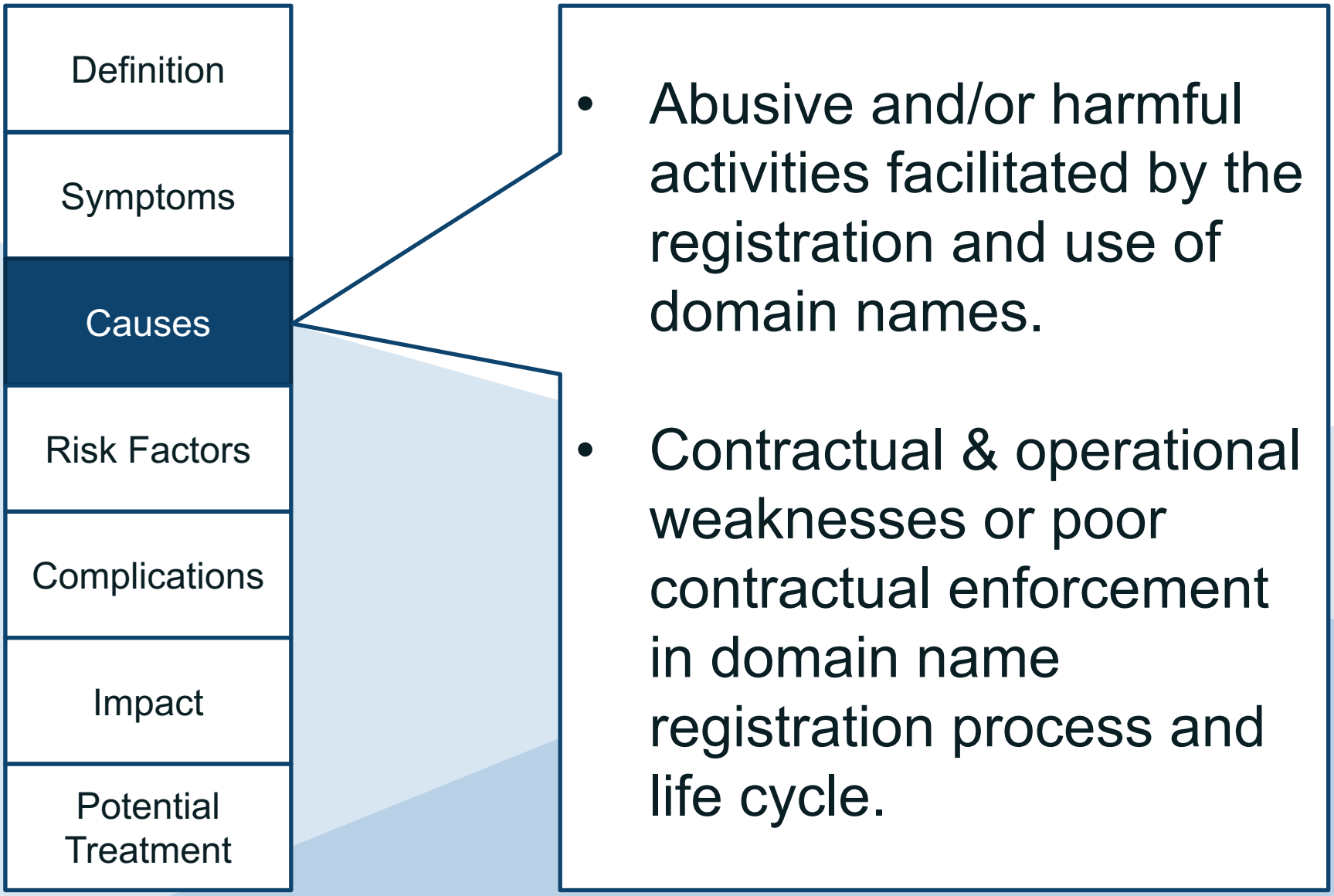
Domain name abuse is the registration or use of a domain name with the capability to cause spam, phishing, malware distribution or command & control of botnets.

Abuse

- Definition
- **Symptoms**
- Causes
- Risk Factors
- Complications
- Impact
- Potential Treatment

Domain names are involved in spam or phishing, and/or are critical to the use of botnet command & control, and/or in the distribution of malware and other nefarious activities.

Abuse


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Abusive and/or harmful activities facilitated by the registration and use of domain names.
• Contractual & operational weaknesses or poor contractual enforcement in domain name registration process and life cycle.

Abuse

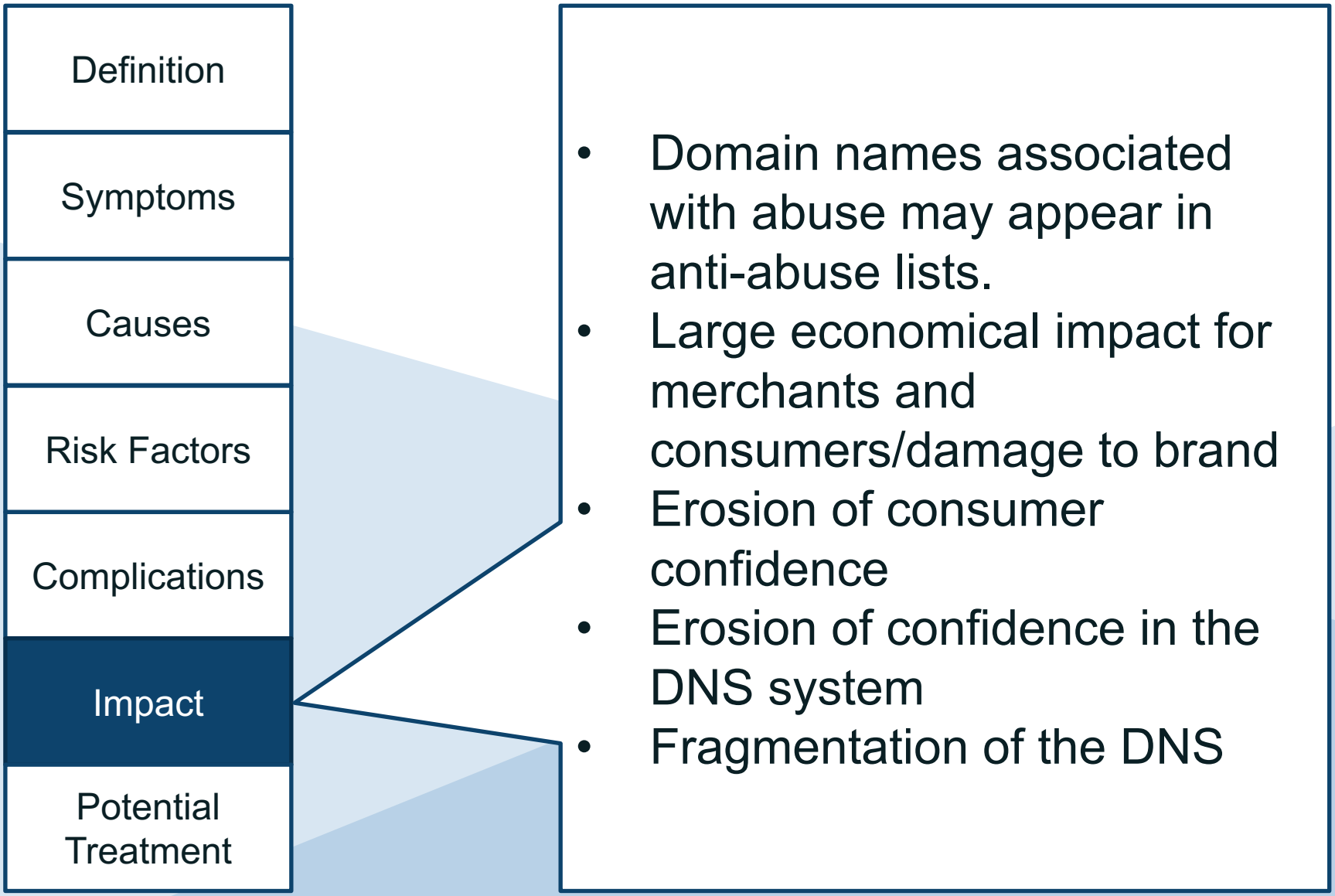
- Nefarious intent of the registrant may not be discovered at the time of registration
- Use of privacy/proxy services
- Incompetent, complacent or complicit behavior of registries/registrars.
- ICANN compliance department rendered ineffective

Abuse

Abuse or criminal activities including but not limited to:

- Phishing
- Botnet Command and Control
- Malware Distribution
- Spam
- …

Abuse


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Domain names associated with abuse may appear in anti-abuse lists.
• Large economical impact for merchants and consumers/damage to brand
• Erosion of consumer confidence
• Erosion of confidence in the DNS system
• Fragmentation of the DNS

Abuse

- Pre-registration automatic screening
- Post registration anti-abuse responses
- Where possible, accelerated procedure for take down
- Common registry/registrar contractual anti-abuse provisions
- Universal minimum price

Excessive Traffic

Excessive Traffic

- Definition
- Symptoms
- Causes
- Risk Factors
- Complications
- Impact
- Potential Treatment

Higher volume of traffic than should be observed in an ideal* world hits DNS servers.

*ideal: no more than a few queries per name per network for the duration of the TTL

Excessive Traffic

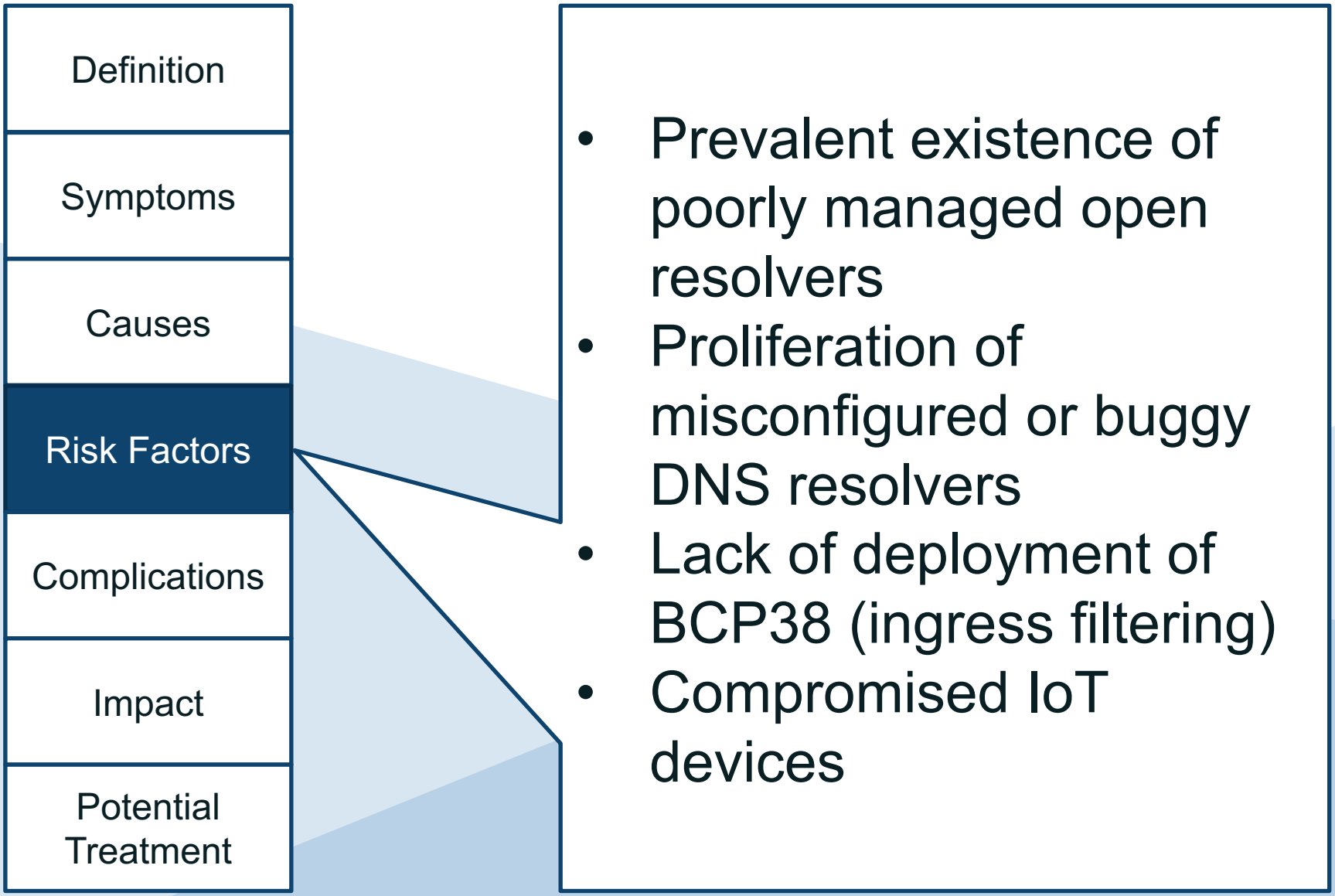
- Definition
- Symptoms
- Causes
- Risk Factors
- Complications
- Impact
- Potential Treatment

- Monitoring systems detect higher than normal traffic
- DNS servers start dropping traffic.

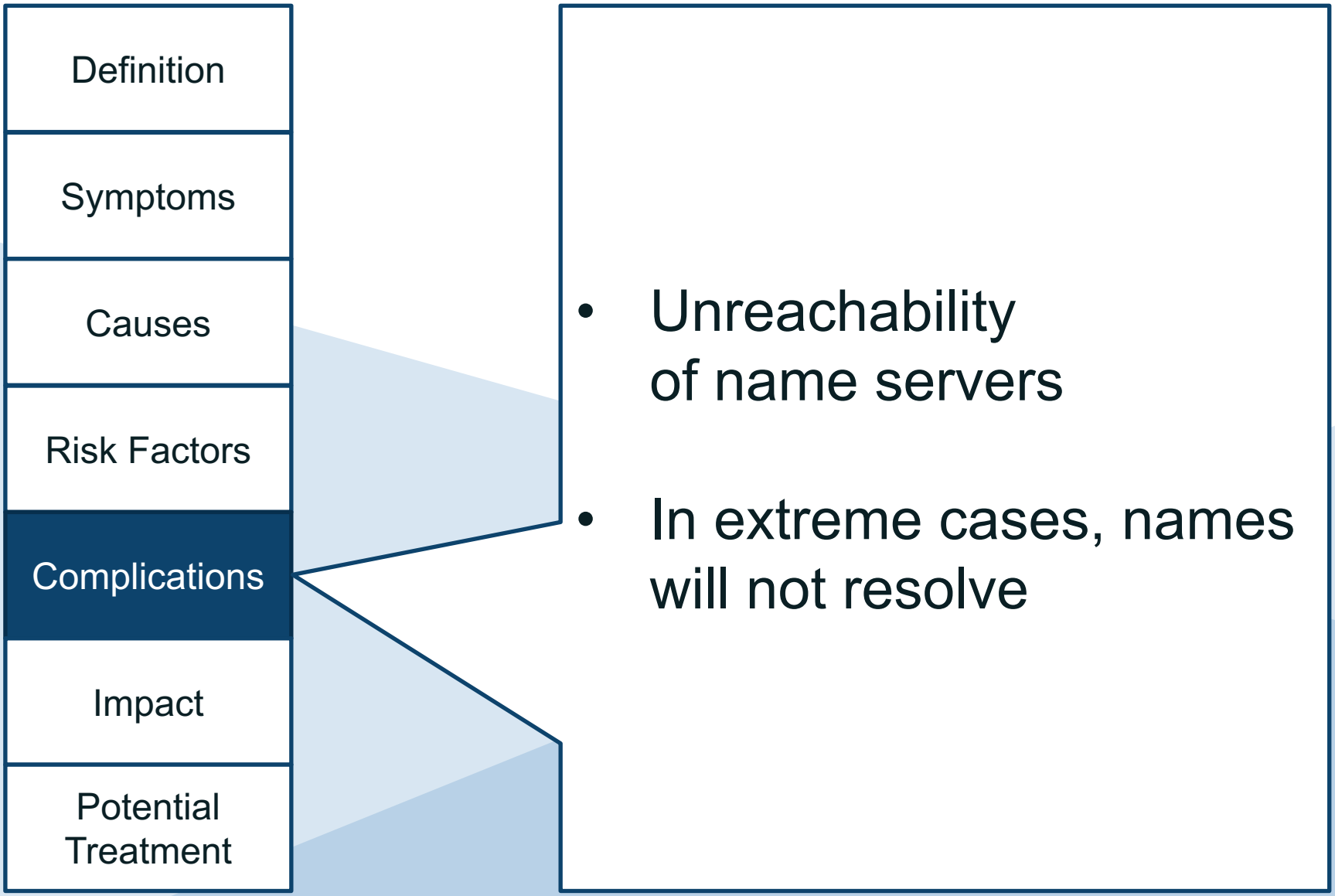
Excessive Traffic

- Many queries are often sent at rapid intervals for the same questions, ignoring TTLs.
- A large number of queries are seen for non-existent names.
- DDOS attacks exacerbate the problem.

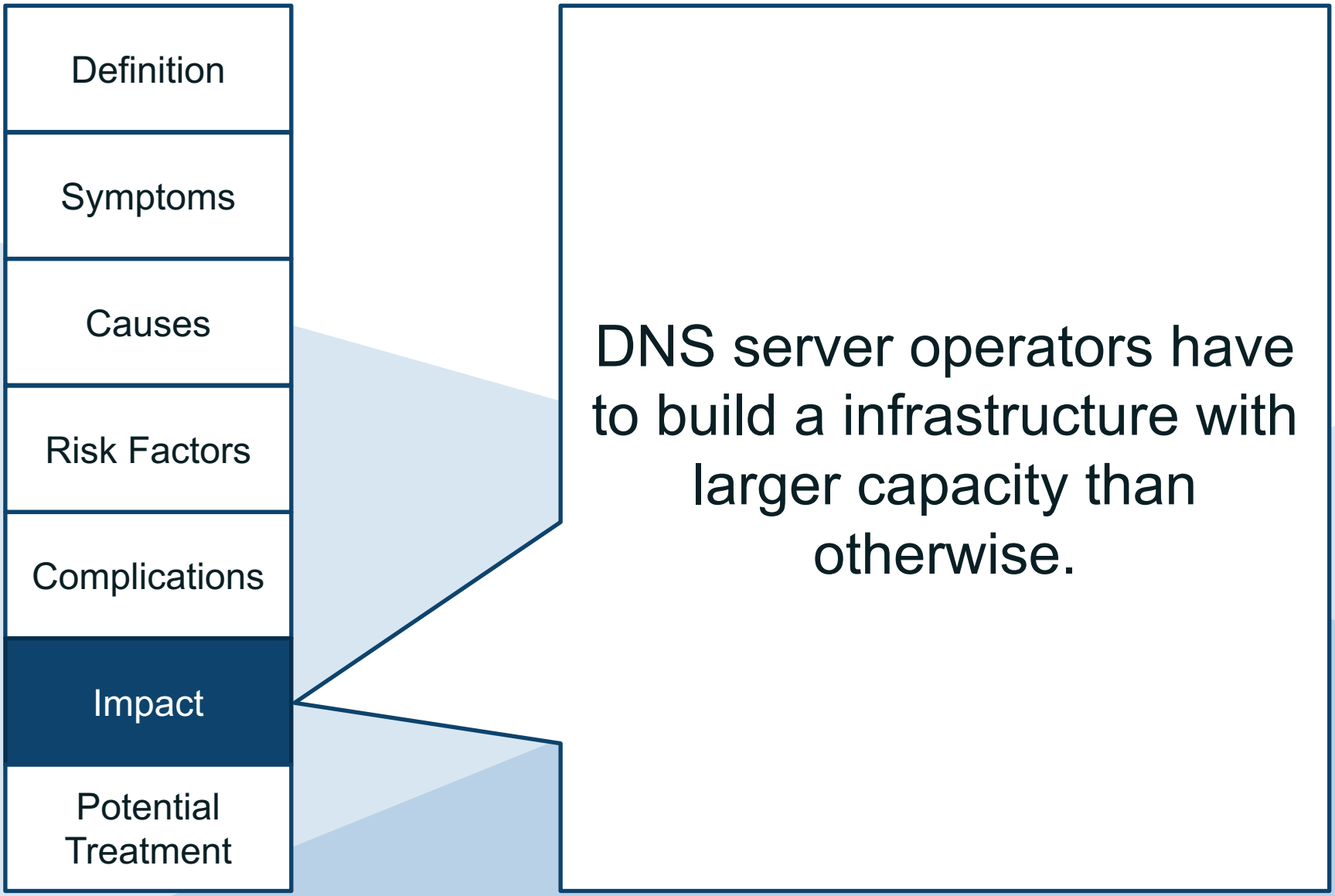
Excessive Traffic



Excessive Traffic



Excessive Traffic



Excessive Traffic

- DDOS mitigation
- Excessive query suppression
- Capacity adaptation

LEAKAGE

LEAKAGE

- Definition
- Symptoms
- Causes
- Risk Factors
- Complications
- Impact
- Potential Treatment

Leakage of private names into the public namespace

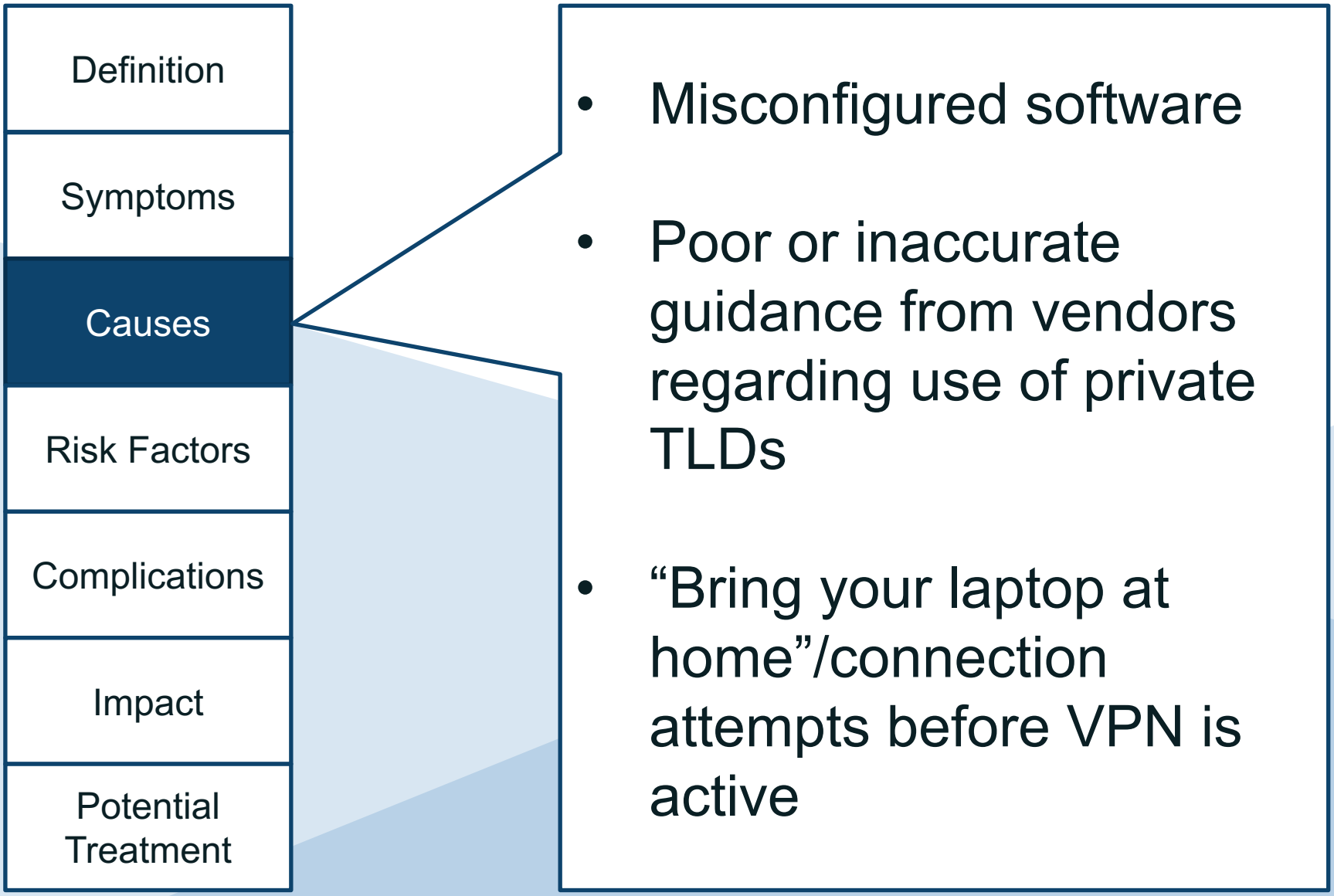
LEAKAGE

- Definition
- Symptoms
- Causes
- Risk Factors
- Complications
- Impact
- Potential Treatment

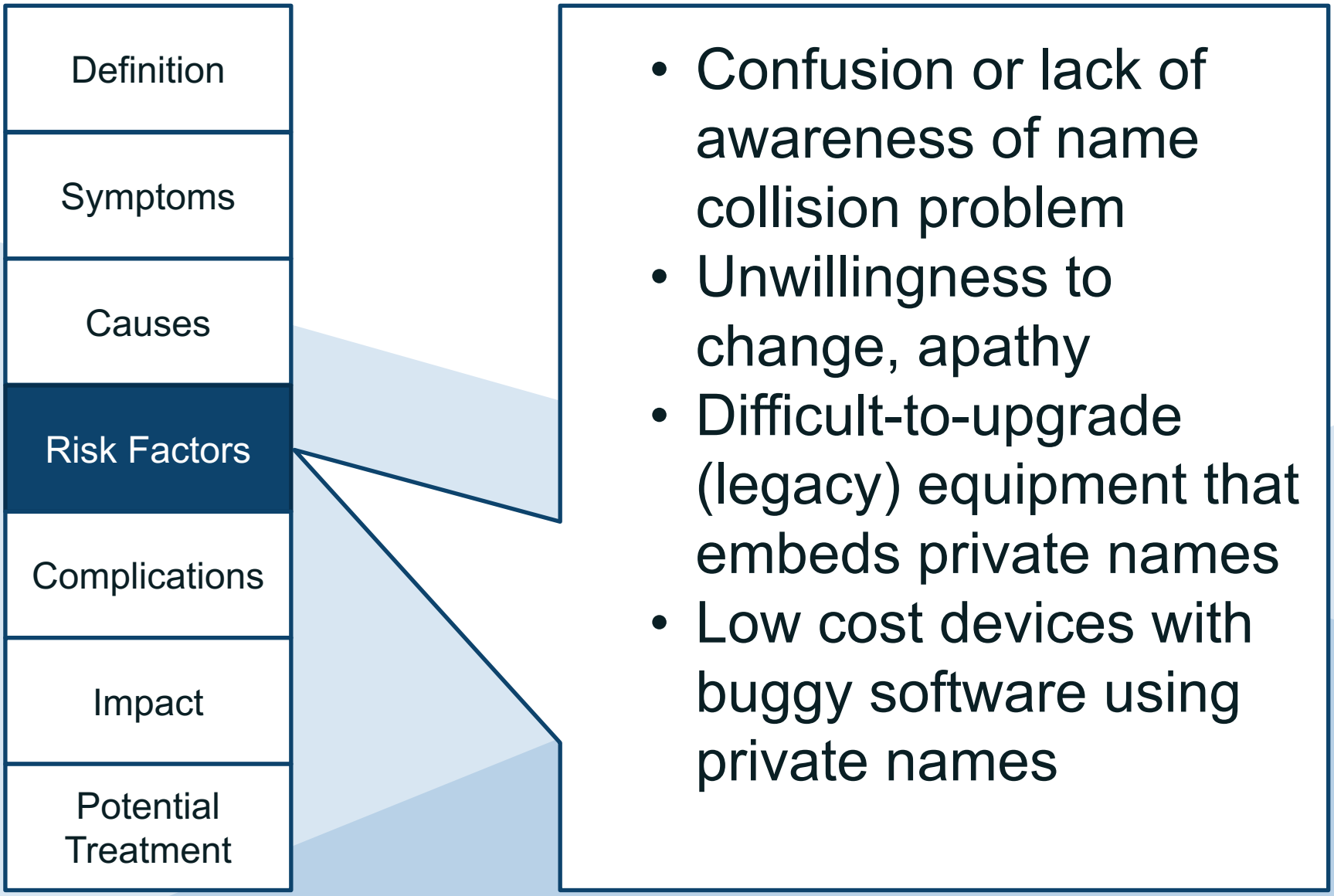
Attempts to resolve private names are observed in the public DNS resolution system

(e.g. .corp, .mail, .home, .wpad, .onion)

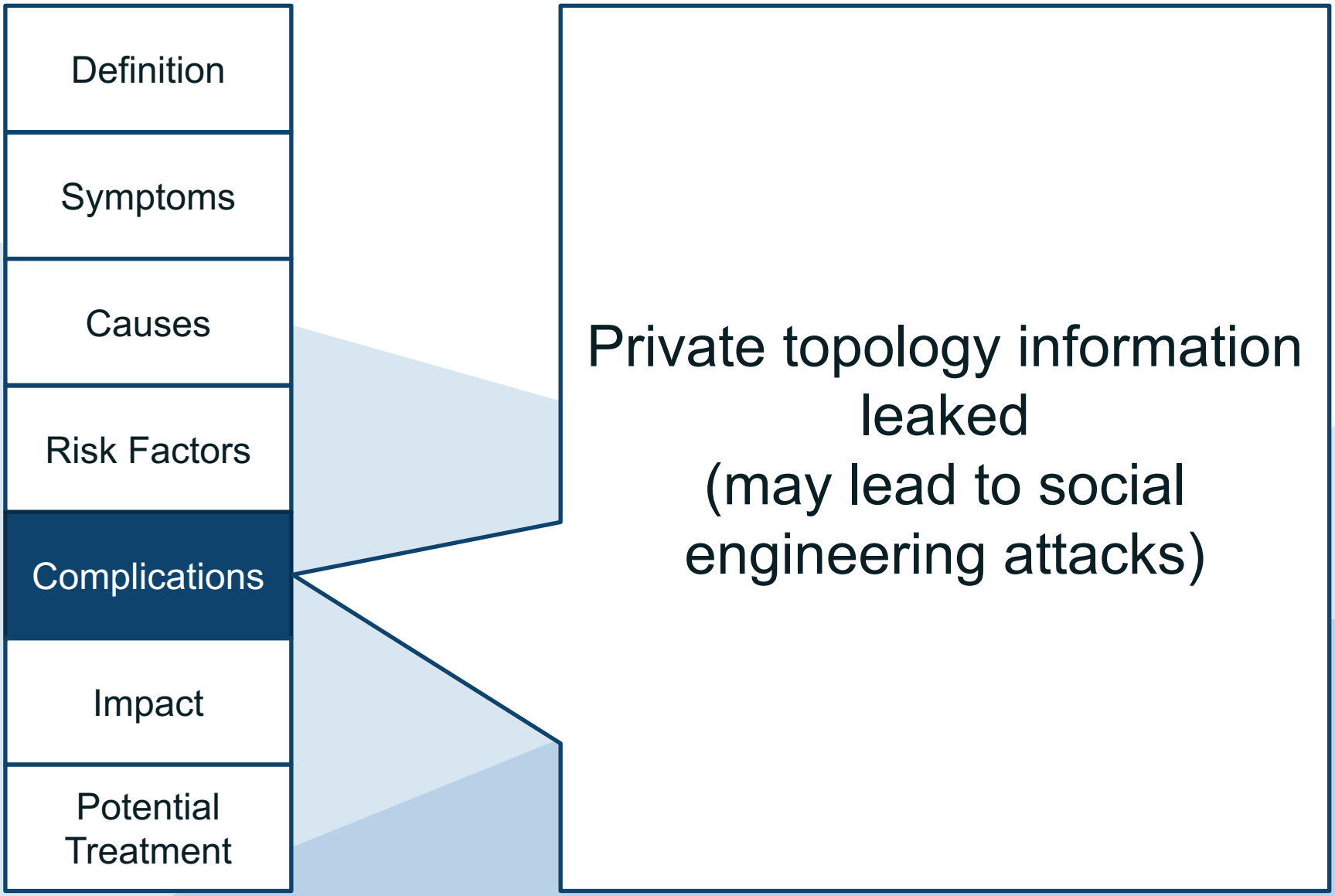
LEAKAGE


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Misconfigured software
• Poor or inaccurate guidance from vendors regarding use of private TLDs
• “Bring your laptop at home”/connection attempts before VPN is active

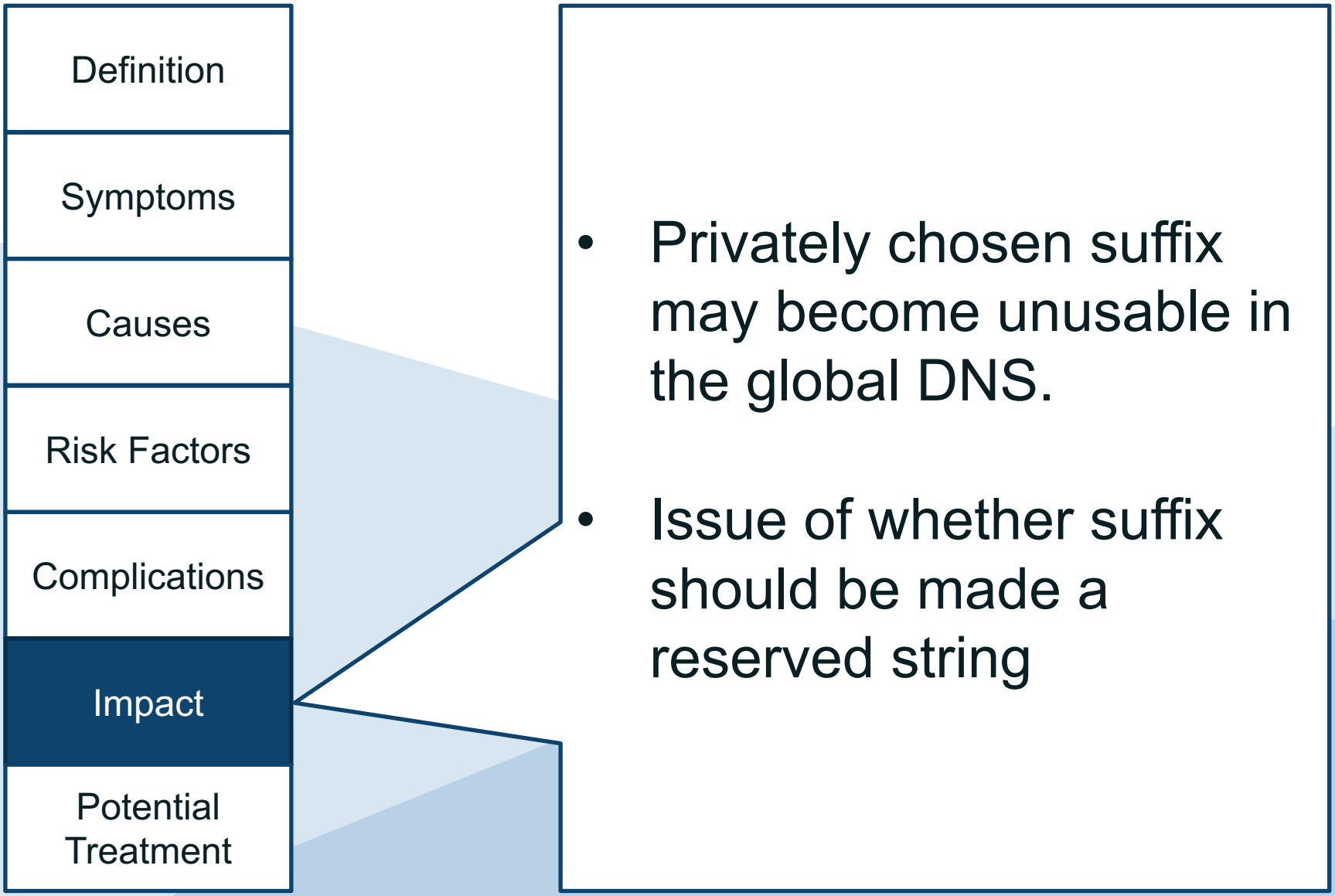
LEAKAGE


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Confusion or lack of awareness of name collision problem
• Unwillingness to change, apathy
• Difficult-to-upgrade (legacy) equipment that embeds private names
• Low cost devices with buggy software using private names

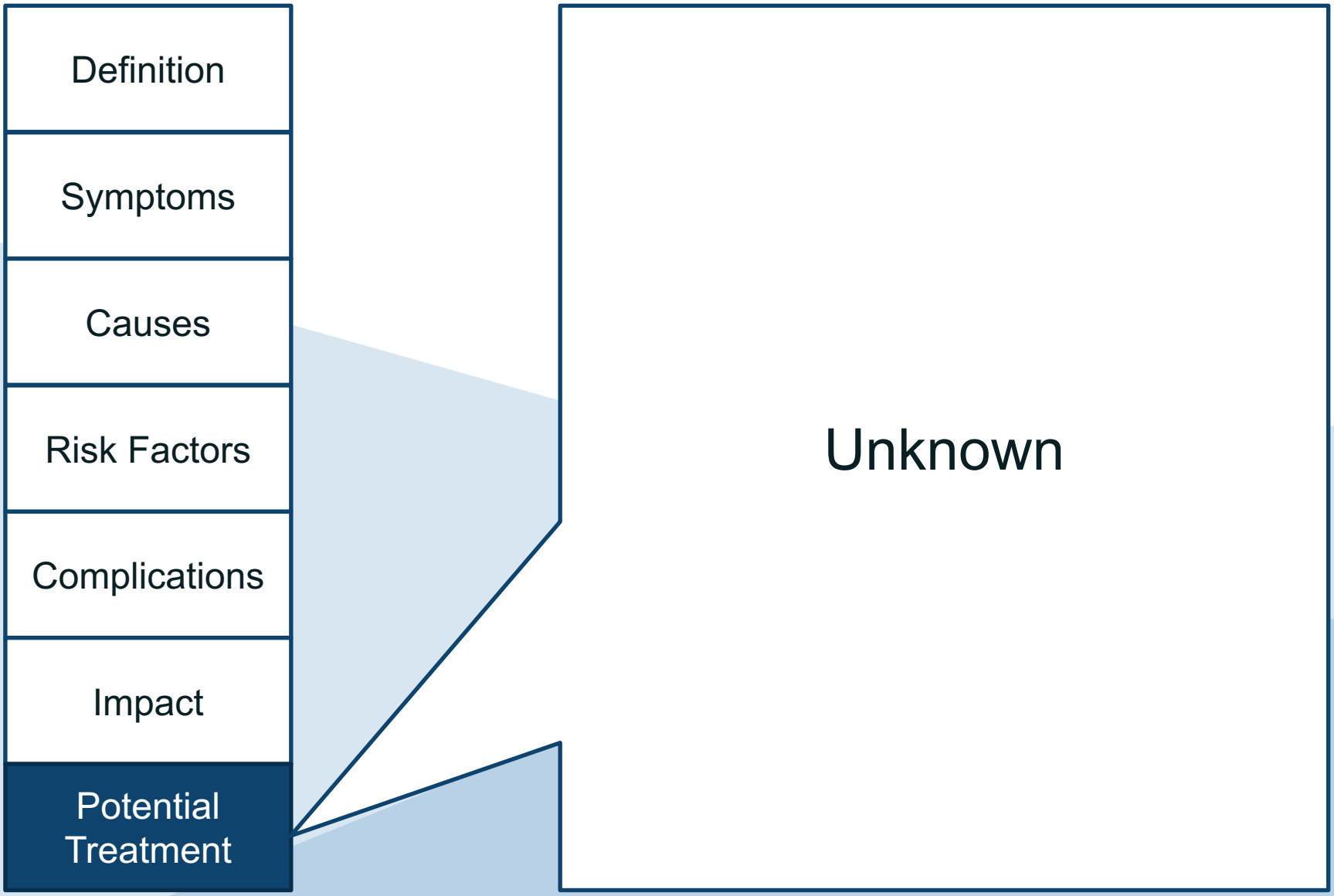
LEAKAGE


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
Private topology information leaked
(may lead to social engineering attacks)

LEAKAGE

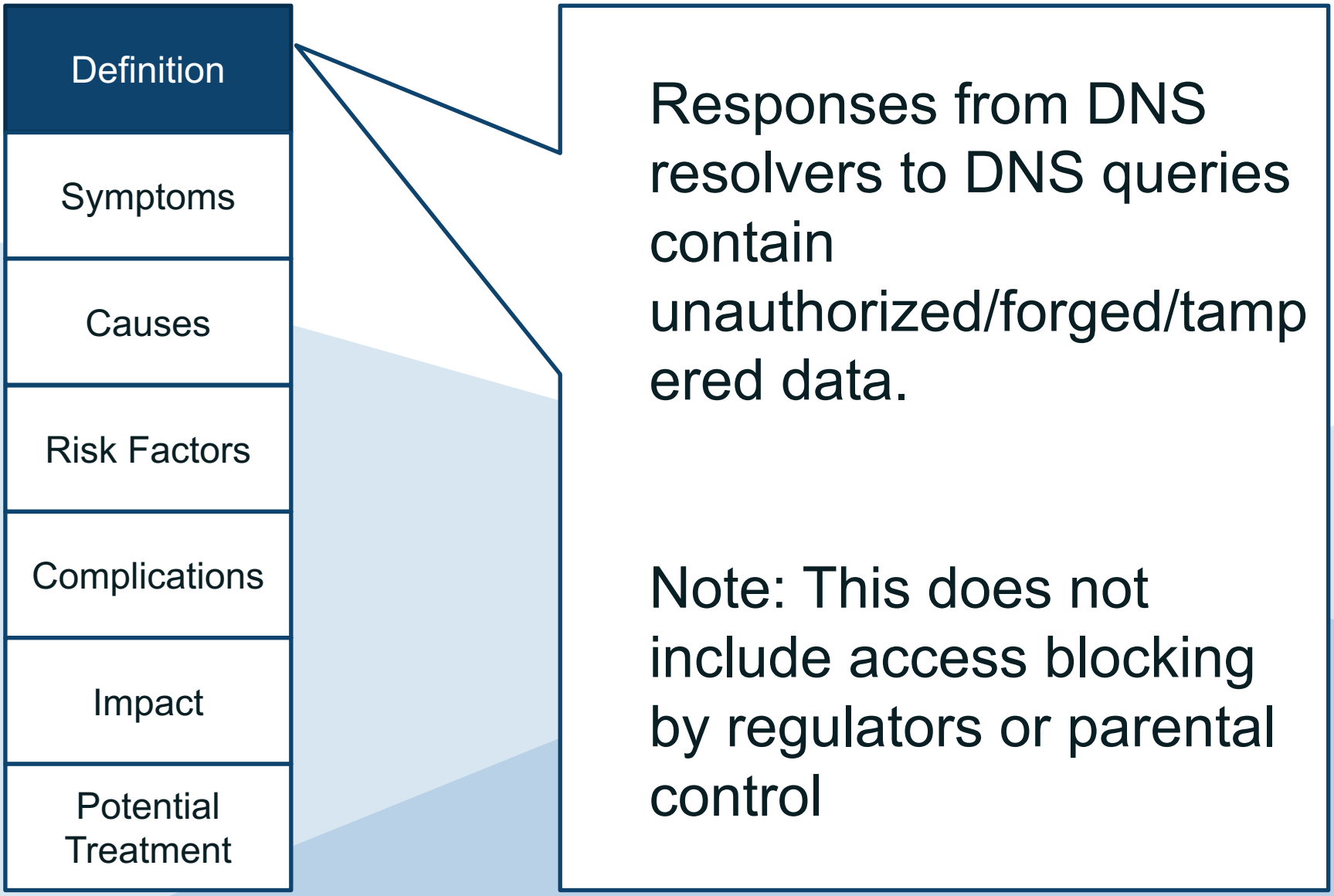

Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Privately chosen suffix may become unusable in the global DNS.
• Issue of whether suffix should be made a reserved string

LEAKAGE


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
Unknown

LIES

Lies

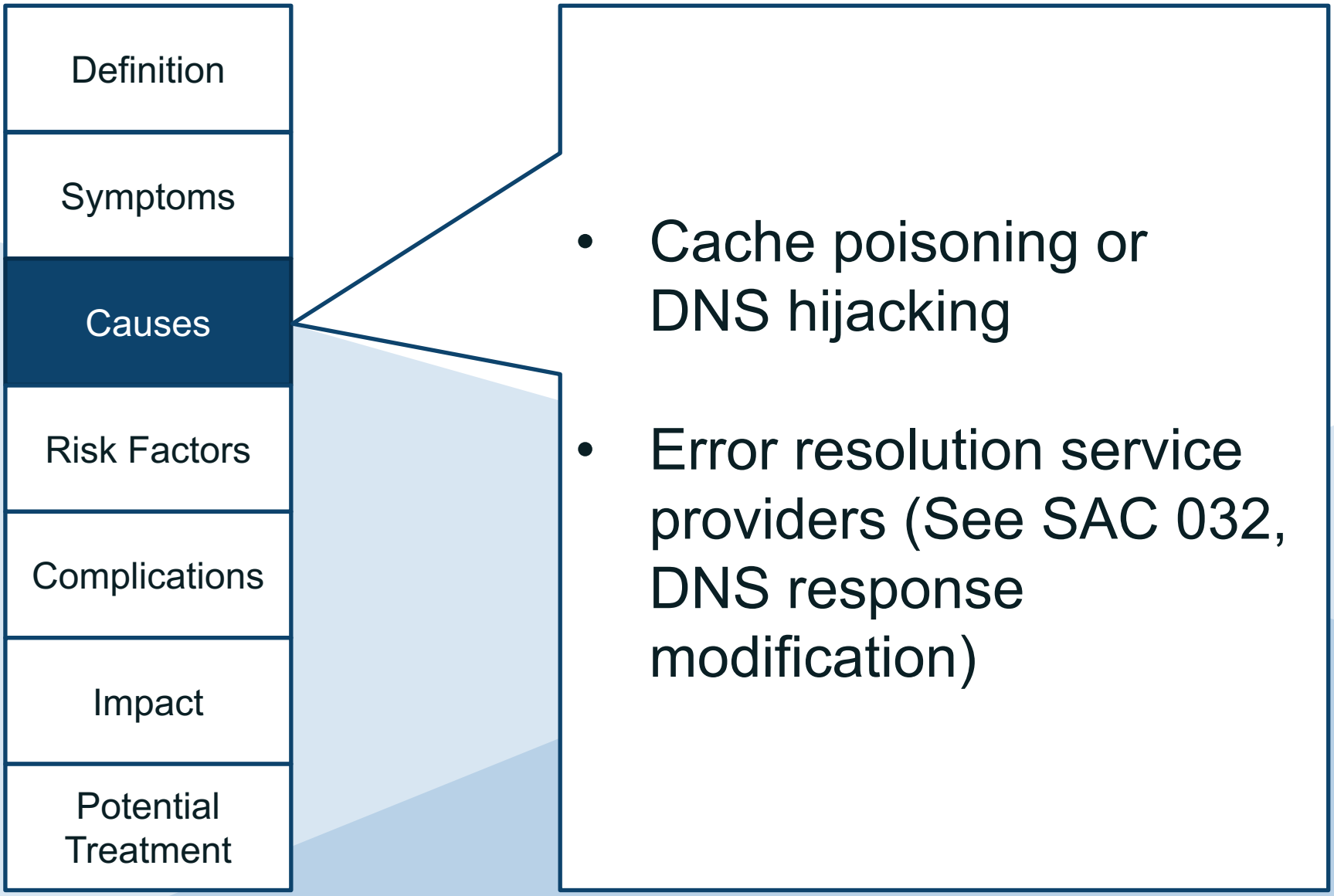

Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
Responses from DNS resolvers to DNS queries contain unauthorized/forged/tampered data.
Note: This does not include access blocking by regulators or parental control

Lies

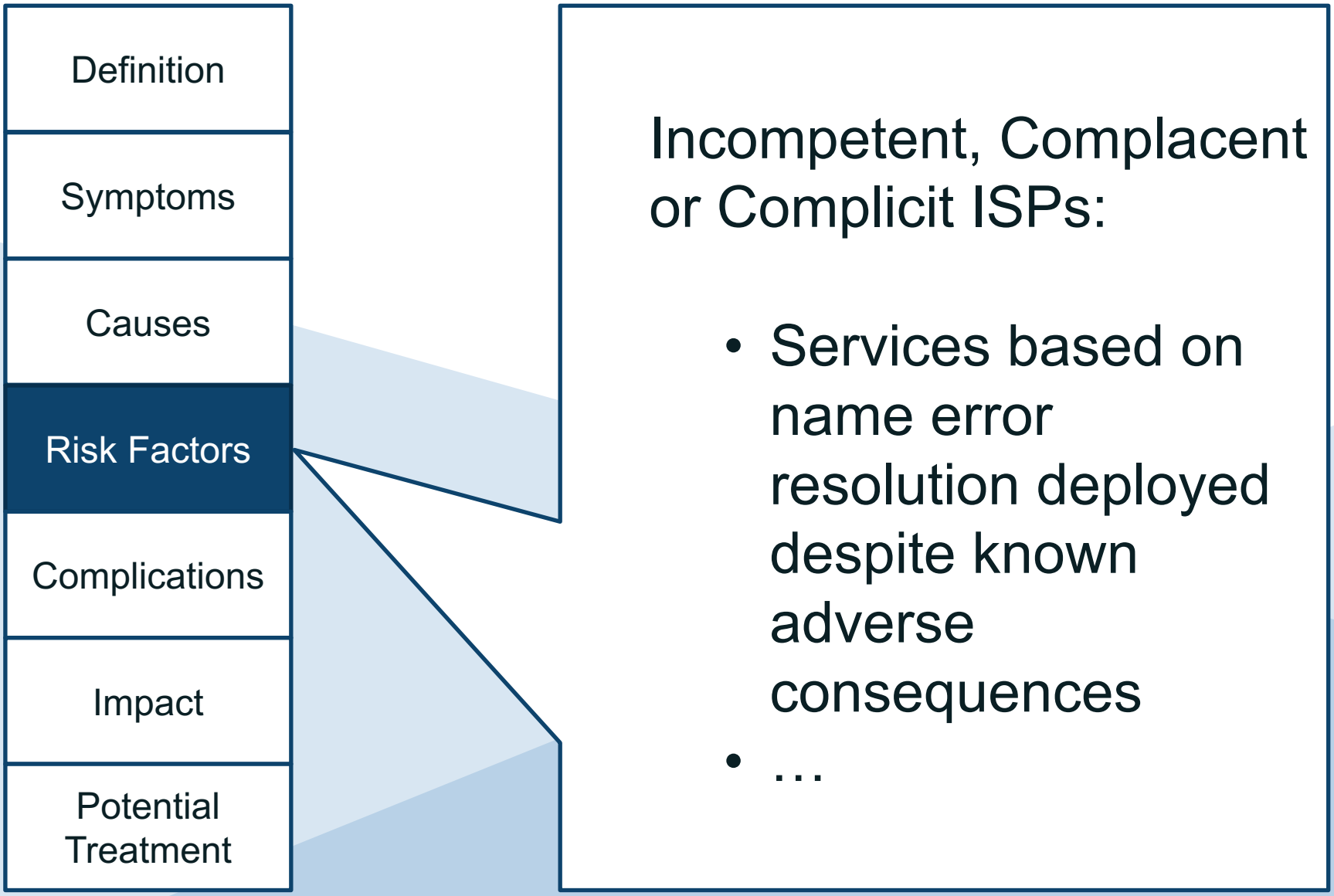
- Definition
- **Symptoms**
- Causes
- Risk Factors
- Complications
- Impact
- Potential Treatment

URLs are re-directed away from intended servers, e.g., to a competitor, malware distribution, phishing, or defacement site.

Lies


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
• Cache poisoning or DNS hijacking
• Error resolution service providers (See SAC 032, DNS response modification)

Lies


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
Incompetent, Complacent or Complicit ISPs:
• Services based on name error resolution deployed despite known adverse consequences
• …

Lies

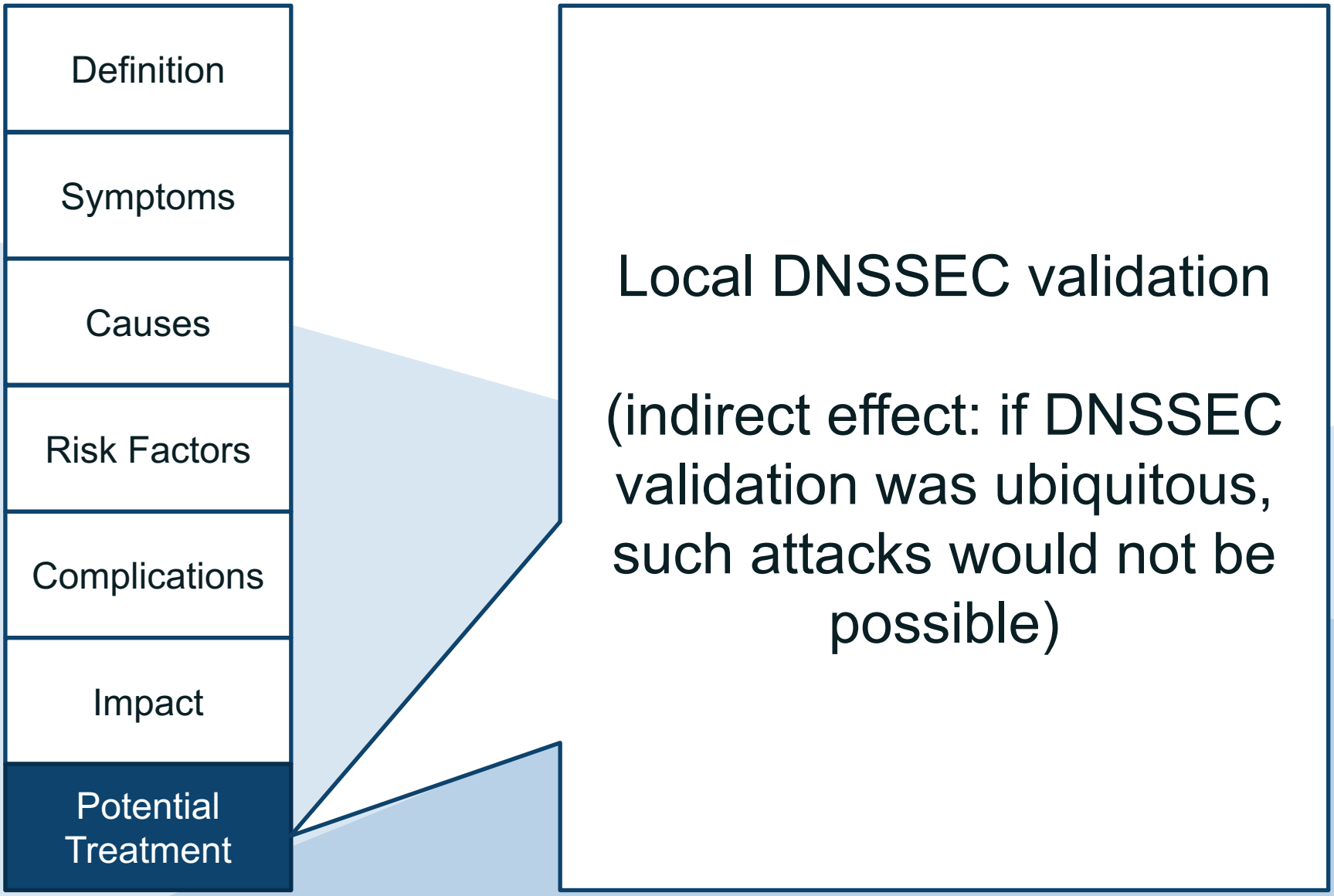
Abuse or criminal activities including but not limited to:

- Malware Distribution
- Phishing, fraud, defacement, hacktivism, DNS or search traffic theft
- Interference with network monitoring or administration (name errors are important to admins!)

Lies

- Loss of business
- Financial loss (from phishing or from response modification that directs revenue-potential traffic to competitor)
- Loss of confidence in the DNS system.

Lies


Definition
Symptoms
Causes
Risk Factors
Complications
Impact
Potential Treatment
Local DNSSEC validation
(indirect effect: if DNSSEC validation was ubiquitous, such attacks would not be possible)

IP Address Problem Areas

Work in Progress,

Done by the RIRs Registry Services

Call for Action

The ICANN ITHI project will soon be working on metrics derived from the problem areas presented in this deck.

We would like to invite DNS experts to work with us to define those metrics.

It is important to get community participation in the early stages of this project to make sure we get this right.

Resources:

Web: http://www.icann.org/ithi
Mailing list: ithi@icann.org
Subscription Page:
https://mm.icann.org/mailman/listinfo/ithi

ITHI Discussion Questions

- Team member questions from ITHI session at DNS Symposium?
- How does ITHI fit into RT's scope?
- Which areas of ITHI are particularly important for RT's consideration?
- Are there areas of risk missing from ITHI?

AOB, Recap of Action Items

Tomorrow's Agenda & Closing Remarks

Review of Agenda – Day Two

1 08:30 – 10:00
Proposed SSR2 Work Approach (James Gannon)

10:30 – 10:40 Break

2 10:40 – 12:30
Work Plan and Timeline

12:30 – 13:15 Review Team Lunch

3 13:15 – 15:15
Subgroup Discussions

15:15 – 15:30 Break

4 15:30 – 16:30
Outreach Plan and Next Steps

5 16:30 – 17:10
Items Requiring Additional Discussion and AOB

6 17:10 – 17:30
Recap of Action Items and Closing Remarks