# Cybersecurity & the ICANN Ecosystem

ATLAS III Preparatory Webinar
22 May 2019

# Today's Presenter

**Patrick Jones**
Senior Director, Global Stakeholder Engagement
ICANN

# Introduction

# Common Elements Inside a Network

**Mail servers**

- E-mail
- Calendaring
- Contacts

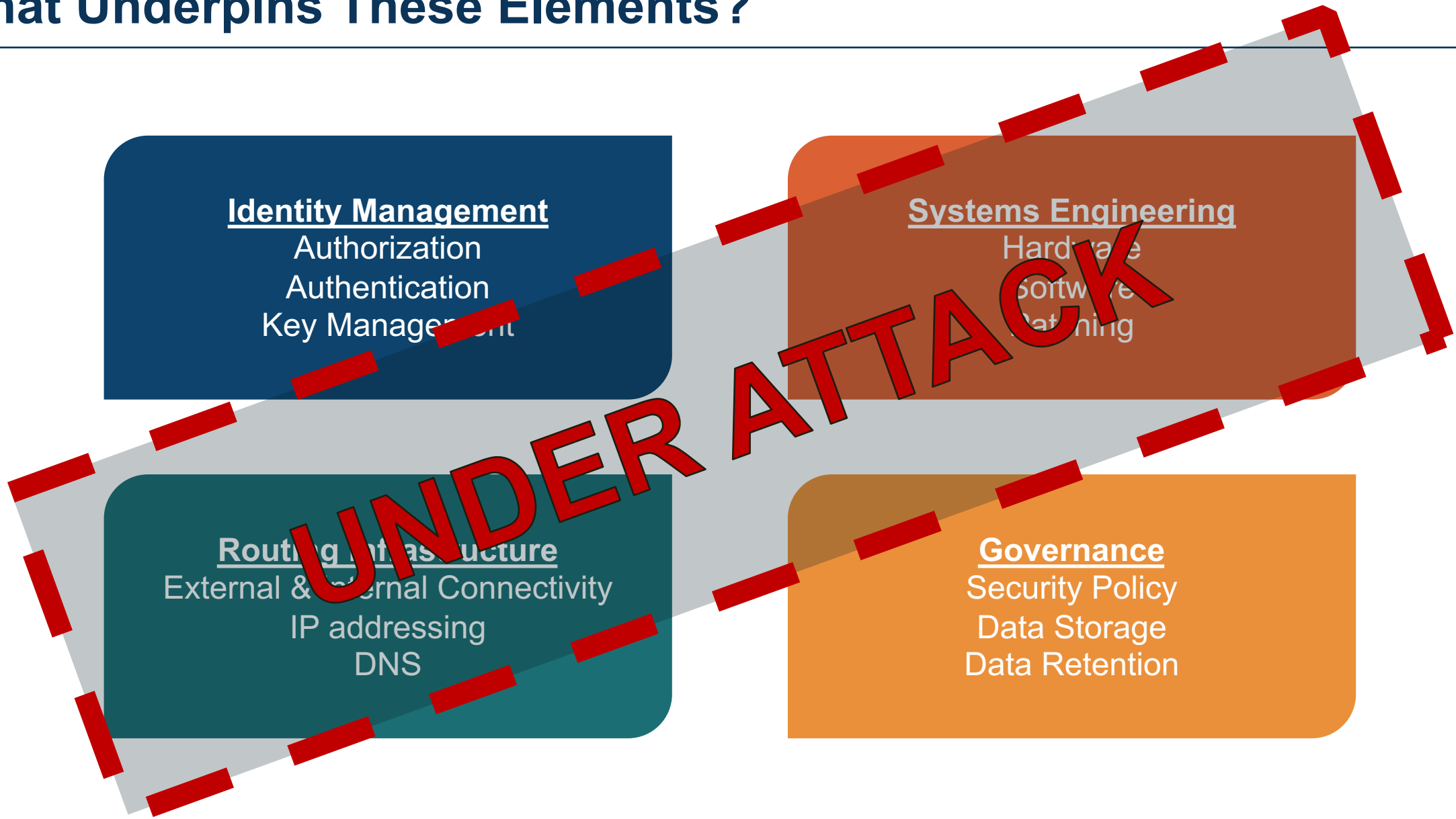
**Database servers**

- Asset data
- Customer data
- Employee data

**File servers**

- Financial information
- Design documents
- Organizational processes and procedures

# What Underpins These Elements?



# Common Types of Cybercrime

**Phishing**

"The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers."

**Malware**

"Software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system"

- e.g., ransomware, key loggers, root kits, viruses

**Botnets**

"A network of private computers infected with malicious software and controlled as a group without the owners' knowledge"

# DNS Abuse

- Everyone uses the DNS to resolve user friendly names to Internet Protocol (IP) addresses
- Disrupt the DNS and you disrupt merchant transactions, government services, social networks
- Exploit the DNS and you can trick, defraud or deceive users
- Vectors for exploitation:
  - Maliciously register domain names
  - Hijack name resolution or registration services
  - Corrupt DNS data

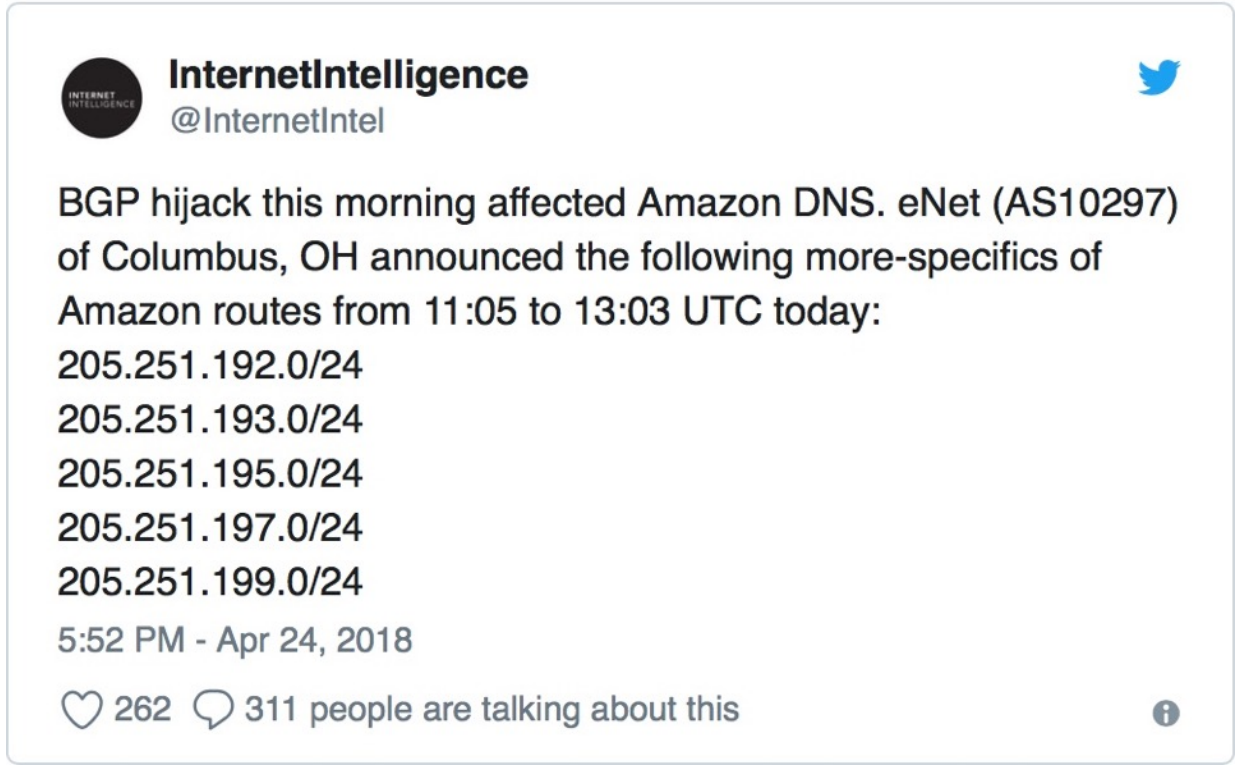
# What do Cyberattacks Look Like?

**We can share two examples of recent cyberattacks. These specific attacks involved:**

- Targeting vulnerabilities in the Internet's routing system
- Targeting vulnerabilities in e-mail systems
- DNS abuse - primarily the surreptitious altering of name resolution

# MyEtherWallet.com

- Route hijacking of Amazon Web Services DNS server addresses to re-direct DNS queries to a nameserver the criminals control
- DNS servers now give out IP address to a fake MyEtherWallet.com website
- Users input login credentials into the fake site
- Attackers steal ~USD21,000,000 of cryptocurrency from the real MyEtherWallet.com using the harvested login credentials



# DNSpionage & Sea Turtle

**DNSpionage** (2018) & **Sea Turtle** (present day)

- “Military cyber-offense prepositioning” – gathering all the intelligence needed to launch military cyber attacks
- 40 organizations in 13 countries in North Africa and the Middle East
- Targeting primarily:
  - National security organizations
  - Ministries of foreign affairs
  - Energy companies
- Infiltrating DNS and e-mail and certificate authorities
  - With all these elements under control, the attackers can obtain and decrypt documents

# ICANN's Role?

- These types of large scale attacks are infrequent, and because of their surface area, involve:
  - Sovereign governments
  - Multi-national companies
  - International law enforcement
  - Widespread news coverage
- Other (smaller scale) cybersecurity incidents happen daily
- The ICANN Community and members of the ICANN Org have a role before, during, and after cybersecurity incidents

***During this webinar we will describe ICANN's role in the cybersecurity ecosystem, and while doing so, help familiarize you with key cybersecurity technologies.***

# ICANN's Role:
# Before a Cybersecurity Incident

# Bylaws

**ICANN's Bylaws place a strong emphasis on cybersecurity**

*"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"*

**Our bylaws include many commitments, including:**

*"Preserve and enhance the administration of the DNS and the operational **stability**, reliability,*

***security**, global interoperability, **resilience**, and openness of the DNS and the Internet"*

# Security, Stability, and Resiliency

**The words we use to describe the cybersecurity framework that ICANN operates in are "security, stability, and resiliency" (SSR)**

- Security means the capacity to protect and prevent misuse of Internet unique identifiers.
- Stability means the capacity to ensure that the system operates as expected, and that users of unique identifiers have confidence that the system operates as expected.
- Resiliency means the capacity of the unique identifier system to effectively withstand malicious attacks and other disruptive events without disruption or cessation of service.

# ICANN's SSR Commitments

In fulfilling our commitments to the SSR of the unique identifier system, ICANN focuses efforts in three arenas:

- Policy development
- Identifier operations
- Capacity Building

# Policy Development: Communities

**Throughout the ICANN ecosystem there are numerous communities developing policies and procedures to improve SSR:**

- GAC's Public Safety Working Group (PSWG)
  - PSWG "focuses on aspects of ICANN's policies and procedures that implicate the safety of the public" including developing the "DNS Abuse and Cybercrime mitigation capabilities of the ICANN and Law Enforcement communities"
- Security and Stability Advisory Committee (SSAC)
  - SSAC engages in ongoing threat assessment and risk analysis of the unique identifier system to assess where the principal threats to stability and security lie
- Root Server System Advisory Committee (RSSAC)
  - Advises the ICANN Board and community on matters relating to the operation, administration, security, and integrity of the Root Server System

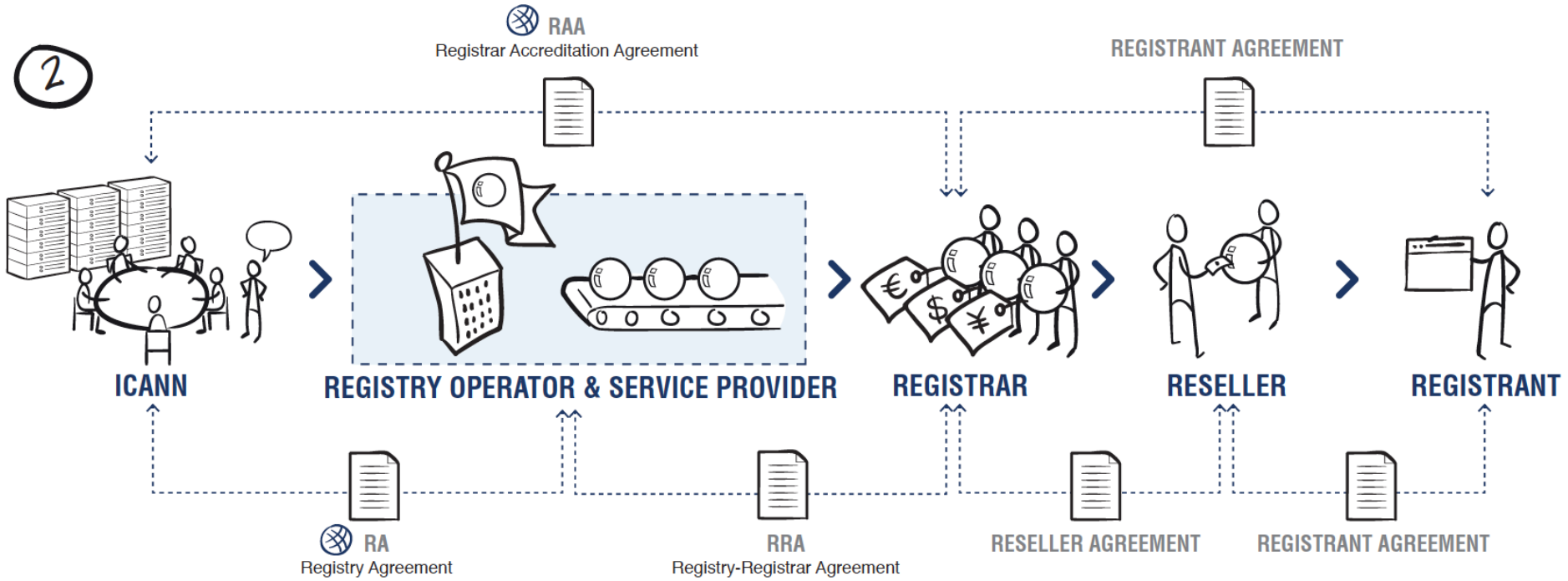
# Policy Development: Contracts

**The contracts between ICANN and registries and registrars are important tools to promote SSR:**

- 2013 Registrar Accreditation Agreement imposes a duty to investigate abuse
- 2017 Registry Agreement includes, for example:

  *"Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision* ***prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law****, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name."*

# Contracted Parties



# Identifier Operations: PTI

**ICANN subsidiary Public Technical Identifiers (PTI) is responsible for the operational aspects of coordinating the Internet's system of unique identifiers**

- Number Resources
  - Allocate IPv4, IPv6, and AS numbers to the RIRs
- DNS Operations
  - Maintain the root zone for forward DNS
  - Administer the .ARPA zone for reverse DNS
  - Maintain the trust anchor for **DNSSEC**
- Protocol Parameter Registries
  - Coordinate over 3,000 registries for IETF protocols

# Identifier Operations: What is DNSSEC?

**Domain Name System Security Extensions (DNSSEC)**

- To help prevent DNS abuse, DNSSEC introduces cryptography that provides assurances to users that DNS data they are seeing is valid and true
- Domain name registrants **SIGN** their DNS data
- DNS operators **VALIDATE** all DNS data passing through DNS resolvers

# Identifier Operations: DNSSEC Keys

**DNSSEC uses Public Key Infrastructure (PKI) technology:**

- The “key signing key” (KSK) is the top-most cryptographic key in the DNSSEC hierarchy.
- The KSK is a cryptographic public-private key pair:
  - Public part is the trusted starting point for DNSSEC validation
  - Private part signs the “zone signing key” (ZSK)
- The KSK builds a “chain of trust” of successive keys and signatures to validate the authenticity of any DNSSEC-signed data.

# Identifier Operations: PTI's Role in DNSSEC

**PTI is entrusted by the Internet to:**

- Issue, manage, change, and distribute DNS keys
- Sign the keyset
- Follow cryptography best practices developed by the Internet Engineering Task Force (IETF)

# Capacity Building

**ICANN staff and community members regularly participate in efforts to teach organizations worldwide on matters relating to the unique identifier system and cybersecurity to increase knowledge and awareness**

- Webinars
- “How it Works” at ICANN meetings
- Technical workshops
- Global law enforcement trainings
- . . . and many other types of capacity building

# ICANN's Role:
# During a Cybersecurity Incident

# Major Actors During a Cyberattack

**Stopping an ongoing cyberattack requires coordinated responses from:**

- Network operators
- Global law enforcement agencies
- National Computer Incident Response Teams (CIRTs)
- Registries

# Attribution

**One of the most important activities during a cyberattack is proper attribution**

- Who is the registrant of the IP addresses used in the attack?
- Who is the registrant of the domain names used in the attack?

**Attribution requires data sources which is the primary role of registration data**

- Registration records for IP addresses and AS numbers (RIRs)
- Registration data for domain names

# ICANN's Coordination Role

**ICANN has a team inside the Office of the CTO (OCTO) that works with organizations during a cyberattack to coordinate responses**

- Deep understanding of cybercrime from both perspectives (attackers and responders)
- Strong connections to global law enforcement and the Internet's OpSec community
- The team uses their deep understanding and their strong community connections to bring all the parties together during takedown efforts

**ICANN has a Coordinated Disclosure Process that security researchers, registries, registrars, and others in the community can use to report vulnerabilities and bugs to ICANN**

# ICANN's Role:
# After a Cybersecurity Incident

# Post Mortem Activities

- Conferences to understand what happened and identify vulnerabilities
  - ICANN DNS Symposium
  - DNS-OARC
  - NOGs
- Adjust the ecosystem to *harden* the Internet against these attacks
  - Policy updates?
  - Contract updates?
  - Protocol (re-)development?
- Community capacity building
  - Network operators
  - Global law enforcement

# Conclusion

# Takeaway: the DNS Really Matters

- The DNS is no longer just a technical function of the network run by system administrators
- The DNS is now a critical infrastructure used in every day communications (e-mail, web browsing, mobile applications) and is a gateway to all your internal systems
- It is critical that policy makers and organization decision makers pay attention to their DNS infrastructure

***If your DNS is compromised, all of your systems and networks are at serious risk***

# Takeaway: New ICANN Recommendations

ICANN **strongly recommends** a set of cybersecurity measures to harden your local DNS infrastructure against attacks

Steps include implementing strong cybersecurity practices for:

- Authorization
- Authentication
- Encryption
- Patching
- E-mail Security

One of the most important recommendations is to implement DNSSEC

See: https://www.icann.org/news/announcement-2019-02-15-en

# Takeaway: The Internet's SSR and ICANN

- Cybersecurity is one area of focus for ICANN's community and for the ICANN org.
- ICANN defines cybercrime to include things like malware distribution, phishing attempts, operating botnets, piracy, and fraudulent or deceptive business practices.
- So much of the time and effort that everyone in the ICANN ecosystem contributes is work intended to increase the stability, security, and resiliency of the Internet and its system of unique identifiers.

# Questions and Answers

**Please ask questions!**

# Engage with ICANN – Thank You and Questions

One World, One Internet

Visit us at **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin/company/icann

slideshare/icannpresentations

soundcloud/icann