INTERNET
INFRASTRUCTURE
COALITION

How Cyber Attacks Create Policy

Christian Dawson

NANOG 69

February 8th, 2017

In This Presentation We’ll Cover

How the U.S. government is looking at cybersecurity.

What the U.S. government considers critical infrastructure.

How the NIST cybersecurity framework may play a role in new requirements.

How Internet providers can take an active role in ensuring good decisions get made.

Cybersecurity in DC Today

In late 2016, the U.S. House Energy and Commerce Committee began a series cybersecurity hearings in response to IoT security problems.

In early 2017, the U.S. Senate Armed Services Committee followed suit, in response to allegations of foreign hacking.

Nov 16, 2016

The House Energy and Commerce Committee on November 15 held a hearing on “Understanding the Role of Connected Devices in Recent Attacks”, to investigate the October 21 DDoS attack on internet backbone provider Dyn.

January 6th, 2017

DHS labeled election equipment as 'critical infrastructure’ over fears of Russian hacking.

This designation requires the Federal government to assess how much regulation, oversight or intrusion the government needs to keep systems safe.

Testimony of James Clapper
Director of National Intelligence, January 7, 2017

Cyber threats:

- Challenge public trust and confidence in global institutions, governance, and norms
- Impose tremendous costs on the global economy.
- Pose an increasing risk to public safety
- Undermine U.S. military and commercial advantage by hacking into U.S. defense industry and commercial enterprises.

January 24th, 2017

The House Energy and Commerce Committee listed cybersecurity oversight as one of their top goals for the 115th Congress

January 30th, 2017

A draft cybersecurity Executive Order being considered by the White House was leaked.

Government Conclusions

Internet service companies are assured to have new responsibilities imposed upon them. Conversations continue on **how extensive** new responsibilities will be, and to whom they will apply.

Internet systems **that connect existing critical infrastructure** may quickly be given new “critical infrastructure” requirements.

What Is Critical Infrastructure?

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and economy - and hence require special Federal oversight, protection and regulation.

What Is Critical Infrastructure?

The Department of Homeland Security (DHS) maintains a list of 16 critical infrastructure sectors:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector

- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Sector-Specific Agencies
- Transportation Systems Sector
- Water and Wastewater Systems

S

How It Works Today

The American Presidential directive PDD-63 of May 1998 set up a national program of "Critical Infrastructure Protection”.

PPD-21 of Feb. 2013 assigned the Department of Homeland Security (DHS)the task of Sector-Specific Agency (SSA) for the IT Sector.

Today’s Information Technology sector-specific plan focuses on a *self-organized, self-run, and self-governed private sector* **“IT Sector Coordinating Council”** to help formulate its plans.

The IT SCC maintains:

The Cyber Storm Exercise Series.

The Software and Supply Chain Assurance (SSCA) Working Group
‘the IT Sector Risk Assessment (ITSRA).

Advocated for voluntary submission to the **NIST Cybersecurity Framework (NIST CSF)**.

What Is The NIST CSF?

In 2014 the NIST Cybersecurity Framework was published. The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations can assess and improve their ability to prevent, detect, and respond to cyber attacks. It "provides a high level taxonomy of cybersecurity outcomes and a methodology to assess and manage those outcomes."

NIST Continued

According to NIST; “The Framework is voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk.

In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders.”

Example NIST Guideline #1

CIS Critical Security Controls (1-5 of 20)

CSC 1: Maintain Inventory of Authorized and Unauthorized Devices.

CSC 2: Maintain Inventory of Authorized and Unauthorized Software.

CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

CSC 4: Maintain Continuous Vulnerability Assessment and Remediation

CSC 5: Maintain Controlled Use of Administrative Privileges.

Example NIST Guideline #2

ISA/IEC-62443 (formerly ISA-99)

A flexible framework to address and mitigate current and future vulnerabilities in industrial automation and control systems (IACS).

1) General: Common or foundational information (concepts, models and terminology) including work products that describe security metrics and security life cycles for IACS.

2) Policies & Procedures: Asset owner information, focused on creating and maintaining an effective IACS security program.

3) System: System design guidance information & requirements for the secure integration of control systems.

4) Component: Work products that describe the specific product development and technical requirements of control system products.

In the coming months and years

Lawmakers in executive and legislative branches are likely to be deciding whether the voluntary NIST CSF is sufficient to be the framework required by parts of the Internet that become considered **Critical Infrastructure**

These Questions Will Likely Be Asked

Is voluntary compliance with existing standards, guidelines, and practices sufficient?

At what point is voluntary not good enough?

What organizations need what standards in order to ensure the safety of the Internet as a whole?

Answers To These Questions

Can change global network health

Can change cost structures

And change who gets to be an Internet provider and who doesn’t.

As Politicians Decide Answers

Internet provider voices can help determine whether their desires are aligned with reality.

Engaged parties will have opportunities to contribute to course corrections.

Consider…

a legislative strategy as part of your cybersecurity, strategy, and your business continuity strategy.

For direct contact with relevant legislators, start here:

https://energycommerce.house.gov/

Additional Resources

To learn more and engage in the conversation:

NIST: ***https://www.nist.gov/***

NIST CSF: ***https://www.nist.gov/cyberframework***

Center for Internet Security: ***https://www.cisecurity.org/***

Cloud Security Alliance: ***https://cloudsecurityalliance.org/***

Internet Infrastructure Coalition: ***https://www.i2coalition.com/***

Q & A

INTERNET
INFRASTRUCTURE
COALITION

Christian Dawson
Executive Director
Internet Infrastructure Coalition
dawson@i2coalition.com
@mrcjdawson