National Cybercrime Strategies

Anthony V. Teelucksingh
U.S. Department of Justice
Chair, OAS/REMJA Working Group on Cybercrime

Council of Europe, Regional Program for the Caribbean, Santo Domingo, Dominican Republic June 10-12, 2019

Element of a National Cybersecurity Framework

- Five elements to a Framework
  - Identify - assets, roles and responsibilities
  - Protect – access controls, encryption, backups
  - Detect - monitoring for unauthorized access
  - Respond – Maintain operations, REPORT TO LE
  - Recover - Repair restore data and operations

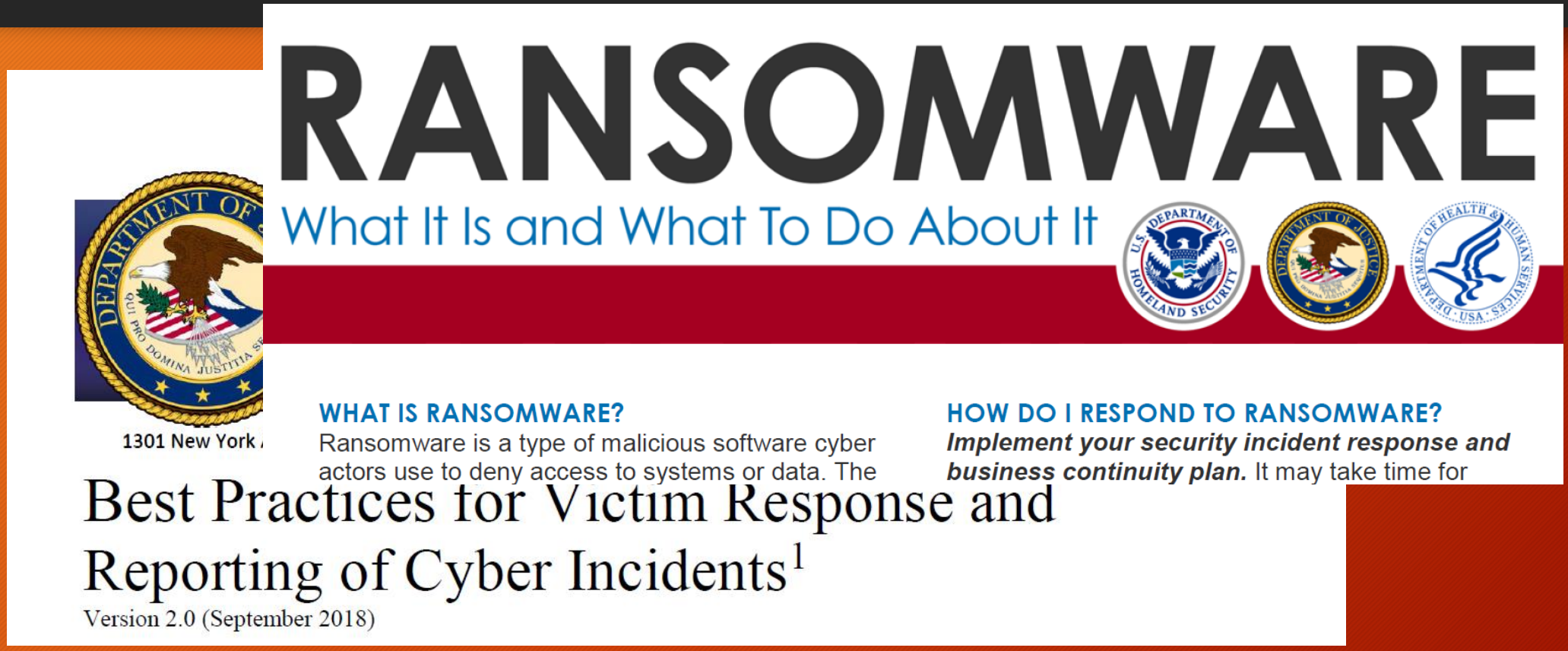
Anti-Cybercrime Needs

- Investigative expertise
  - Specialized investigators in cybercrime in every federal criminal investigative agency, including digital forensic capability
- Prosecutorial expertise
  - Specialized prosecutors in cybercrime in every U.S. Attorney's office in 91 federal districts
- Judicial Education
- Public awareness
- "Prevent, detect, disrupt, and investigate cyber threats"

Computer Crime and Intellectual Property Section

- Prosecute violations of cybercrime and intellectual property crime
  - 44 prosecutors at full strength
- Provide training to federal law enforcement
  - Also outreach to industry and state law enforcement
- Represent the U.S. in international fora on cybercrime
  - Council of Europe, OAS, United Nations
  - UNODC Intergovernmental Experts Group on Cybercrime
- Policy role
  - Propose and comment on legislation
  - Newly created Cybersecurity Unit

Cybersecurity Unit



RANSOMWARE

What It Is and What To Do About It

1301 New York

WHAT IS RANSOMWARE?

Ransomware is a type of malicious software cyber actors use to deny access to systems or data. The

HOW DO I RESPOND TO RANSOMWARE?

Implement your security incident response and business continuity plan. It may take time for

Best Practices for Victim Response and Reporting of Cyber Incidents[1]

Version 2.0 (September 2018)

U.S. National Cybercrime Strategy

- Improve incident reporting
  - Prompt reporting to law enforcement important for a timely response
- Modernize electronic surveillance and computer crime laws
  - Update legal framework as necessary
- Reduce threats from transnational criminal organizations
  - Provide the procedural and forensic tools to investigate international crime
- Improve apprehension of criminals located outside the U.S.
  - Deterring cybercrime requires a credible threat that perpetrators will be arrested

U.S. National Cybercrime Strategy

- Improve apprehension of criminals located outside the U.S.
  - Deterring cybercrime requires a credible threat that perpetrators will be arrested
- Capacity-building for partner countries
  - Support effective solutions for efficient cross-border information sharing
  - Encourage use of existing international tools like the UNTOC and the 24/7 network points of contact
  - Expand the international consensus on the Budapest Convention

U.S. International Strategy Overview

- U.S. goal is to combat transnational cybercriminal activity anywhere in the world that targets U.S. persons, corporations, or assets
  - Includes state actors which target U.S. corporations
- Strengthen relationships with international law enforcement partners
- Provide capacity-building assistance on request to U.S. partners
- Promote the Budapest Convention as an essential tool for international cooperation