RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: PNG-R09

Human Dimensions of Active Defense

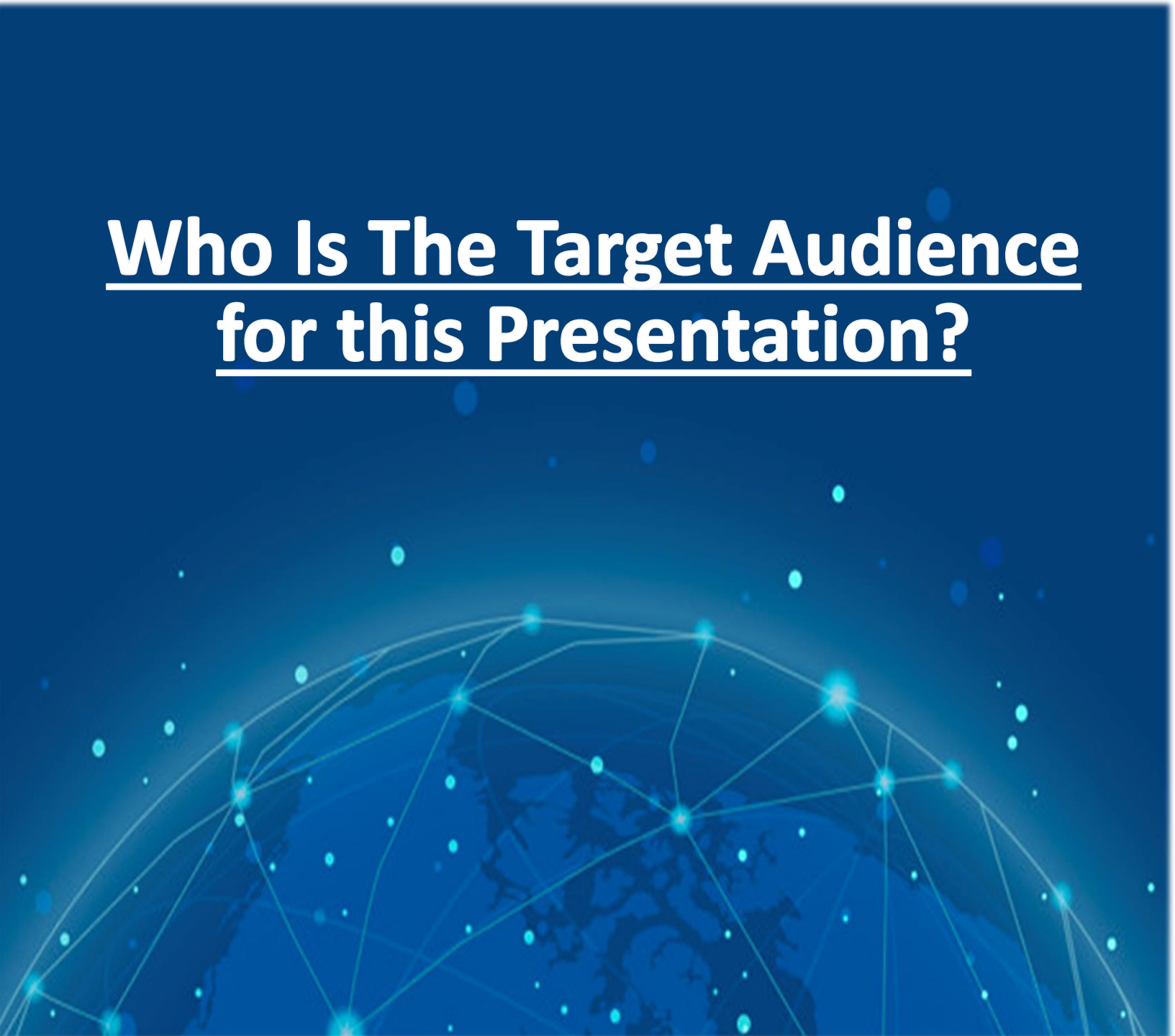
Leonard Bailey

Head of Cybersecurity Unit/Special Counsel for National Security
U.S. Department of Justice, Criminal Division
Computer Crime & Intellectual Property Section

By the time we're done, you'll know …

- How to use these types of active defense discriminately, intelligently, and lawfully.
- What you need to do to be prepared to conduct these types of active defense activities.
- How law enforcement can play a role in your planning.

Who Is The Target Audience for this Presentation?



- The private Sector, not the government.
- Gatherers of cyber threat intelligence
- Organizations that hire cyber threat intelligence gatherers
- Victims attempting to recover their stolen data
- Organizations purchasing malware

DOJ's Computer Crime & Intellectual Property Section

Interpreting the Relevant Laws: CFAA & Electronic Surveillance Laws

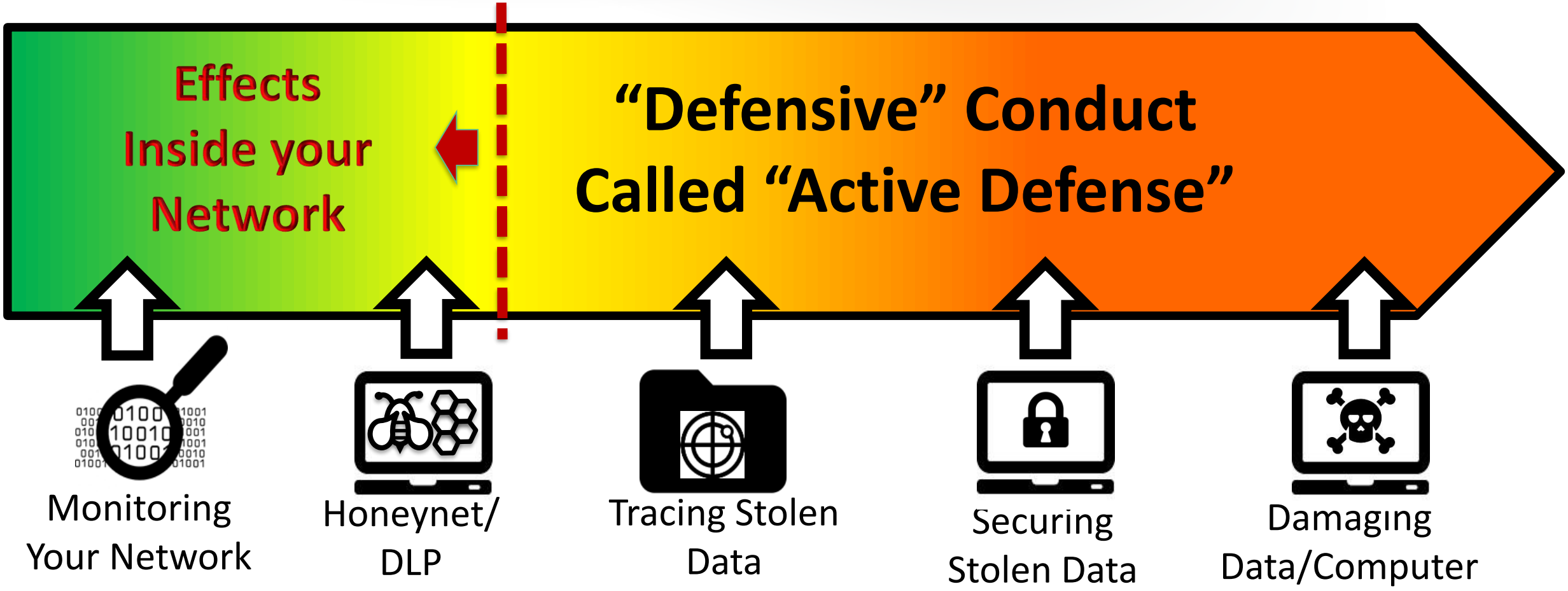
Prosecuting Computer Crime Cases with U.S. Attorney's Offices

Outreach to Industry to Encourage Good Cybersecurity Practices

RSAConference2020

“Active Defense” from DOJ’s Perspective

Active Defense: Technical Operations

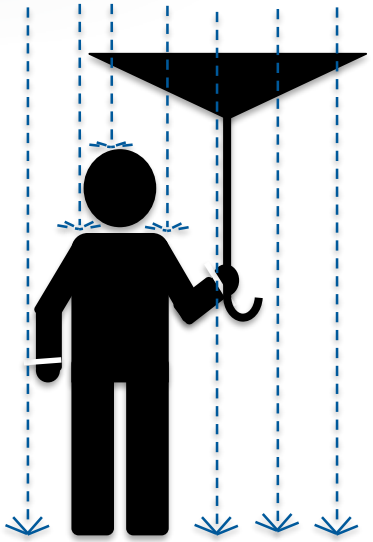


U.S. Department of Justice
Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division

Hack Back: The Problems

Reason 3:
No Law Enforcement Deconfliction

Reason 1:
Escalation



Reason 2:
Ineffectiveness

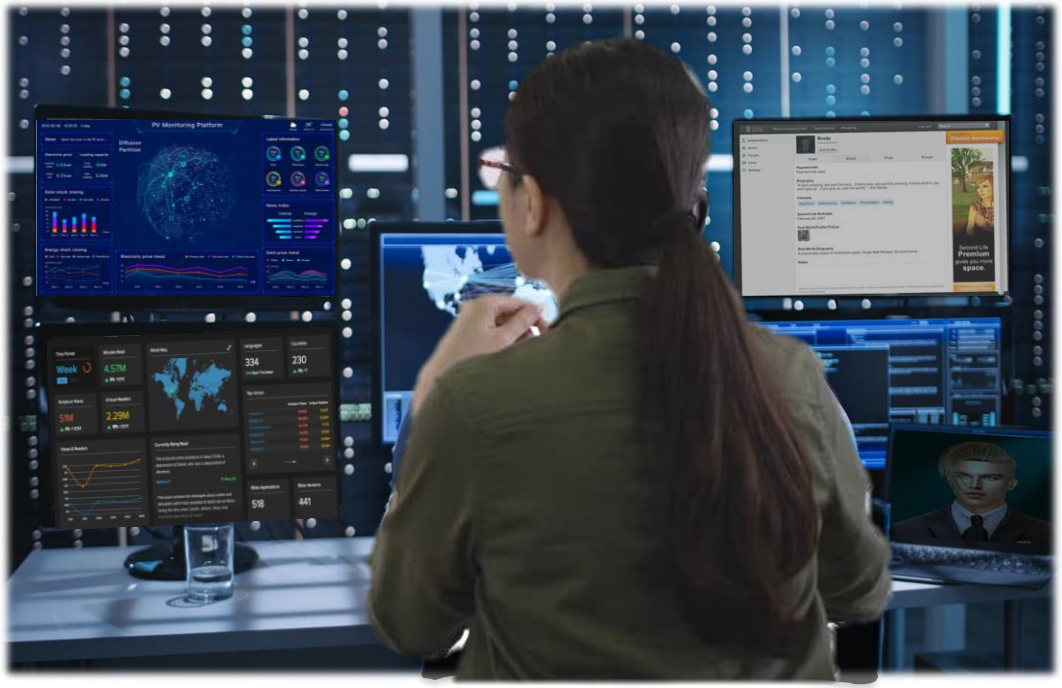
U.S. Department of Justice
Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division

Two Rules of Active Defense

Don’t Become a Victim!

Don’t Become a Perpetrator!

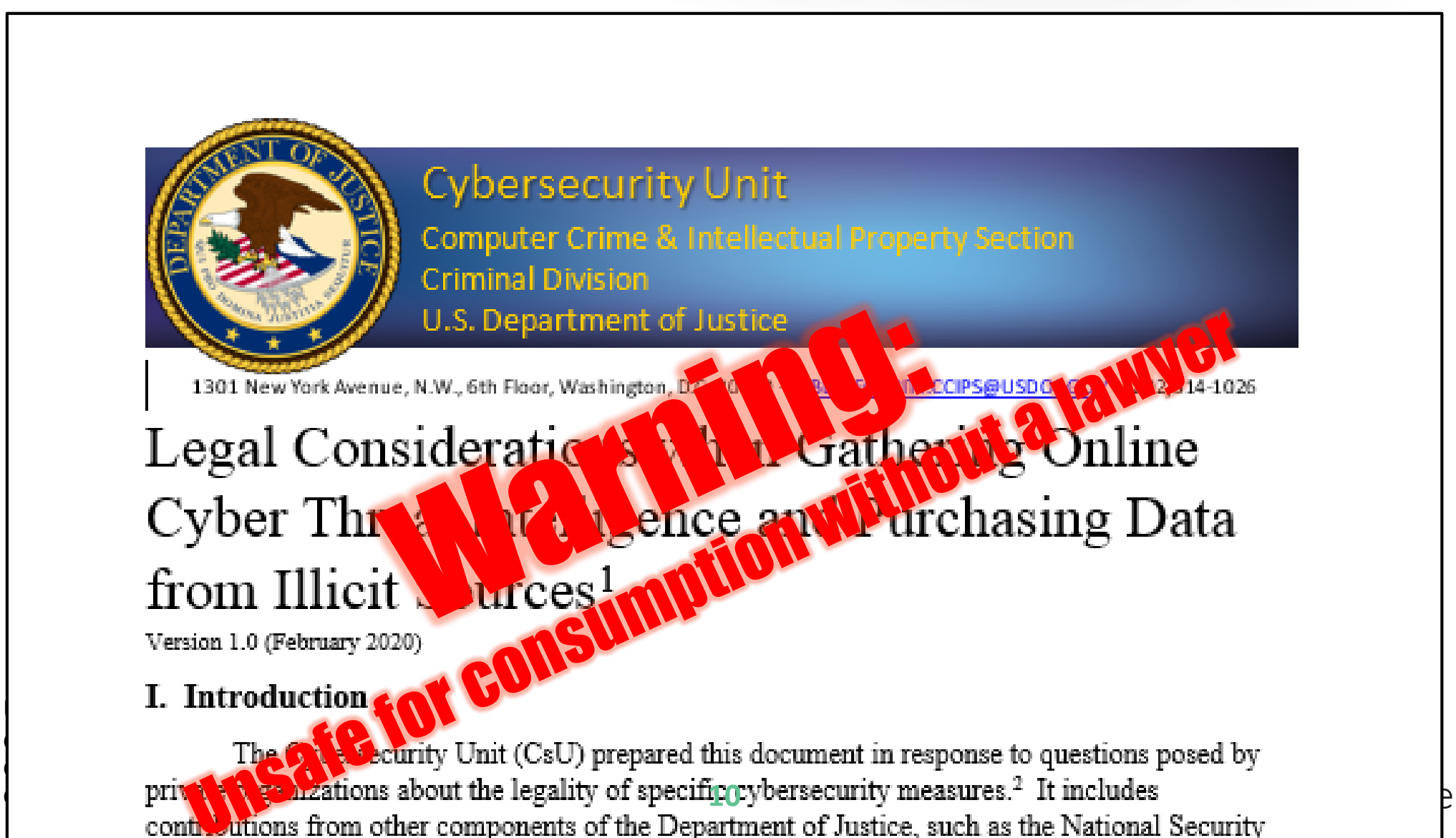
Human-Directed Active Defense



Cyber Threat Intelligence Gathering

Re-Acquiring Stolen Data & Buying Malware or Vulnerabilities

Human-Directed Active Defense



Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D[illegible] CCIPS@USDOJ.G[illegible] 14-1026

Legal Considerations [illegible] Gathering Online Cyber Thr[illegible]gence and Purchasing Data from Illicit Sources[1]

Version 1.0 (February 2020)

I. Introduction

The Cybersecurity Unit (CsU) prepared this document in response to questions posed by private organizations about the legality of specific cybersecurity measures.[2] It includes contributions from other components of the Department of Justice, such as the National Security

RSAConference2020

Human Directed Active Defense:
Intelligence Gathering

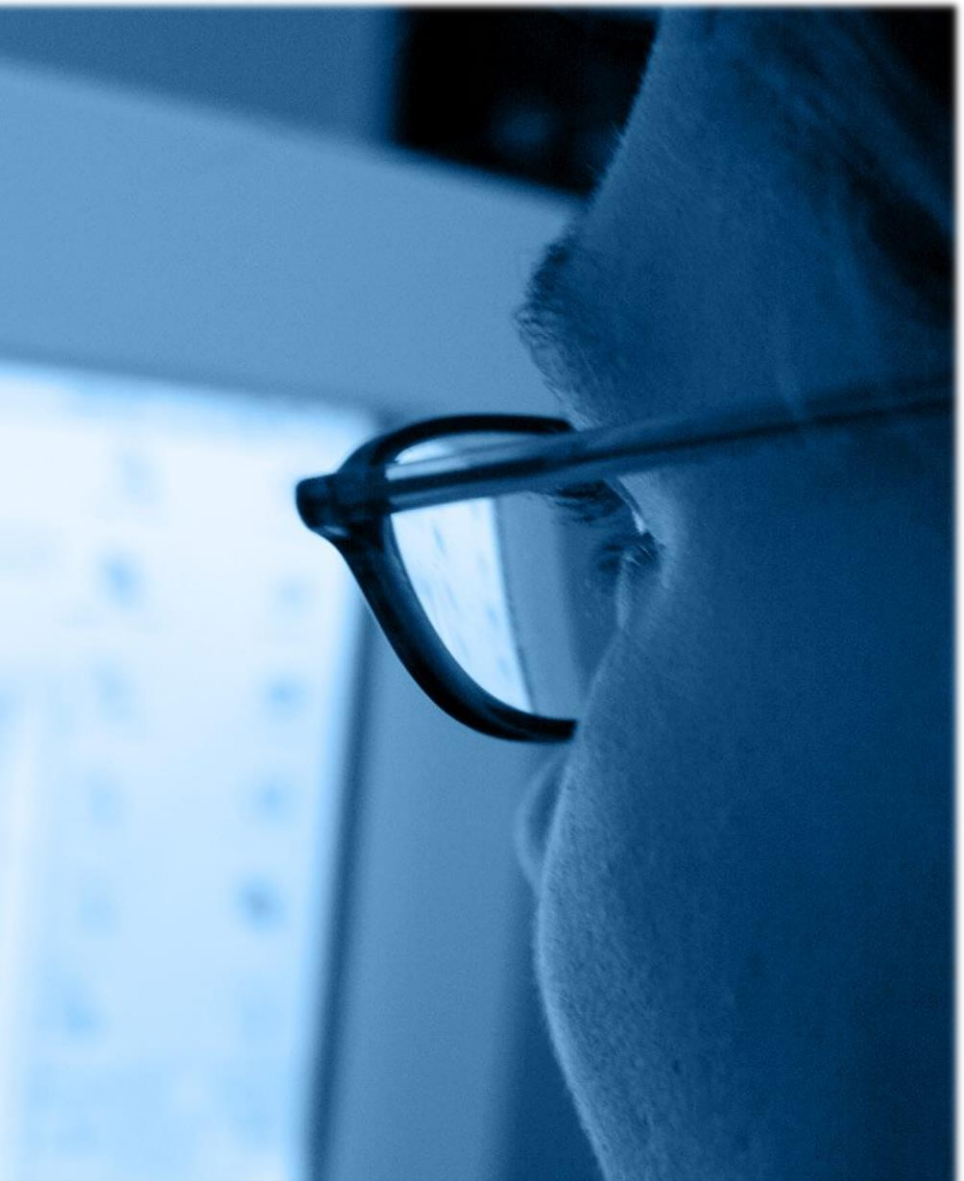
What you think you sound like.

What you probably sound like.

Scenario Assumptions

- The collector does not have criminal intent
- The forums targeted for collection are sites on which criminal activity is planned and conducted
  - TTPs are traded for purposes of facilitating computer crime
  - The forum focuses exclusively on commission of computer crime and not other crimes (e.g., child pornography or terrorism)
- Access to the forum was secured lawfully
  - Deception (e.g., a fake identity) generally maybe used
  - Stolen credentials or a technical exploit may not
- If a fake identity was used, it was not an assumed identity of a real person or someone with a special status

Intelligence Gathering: Just Lurking

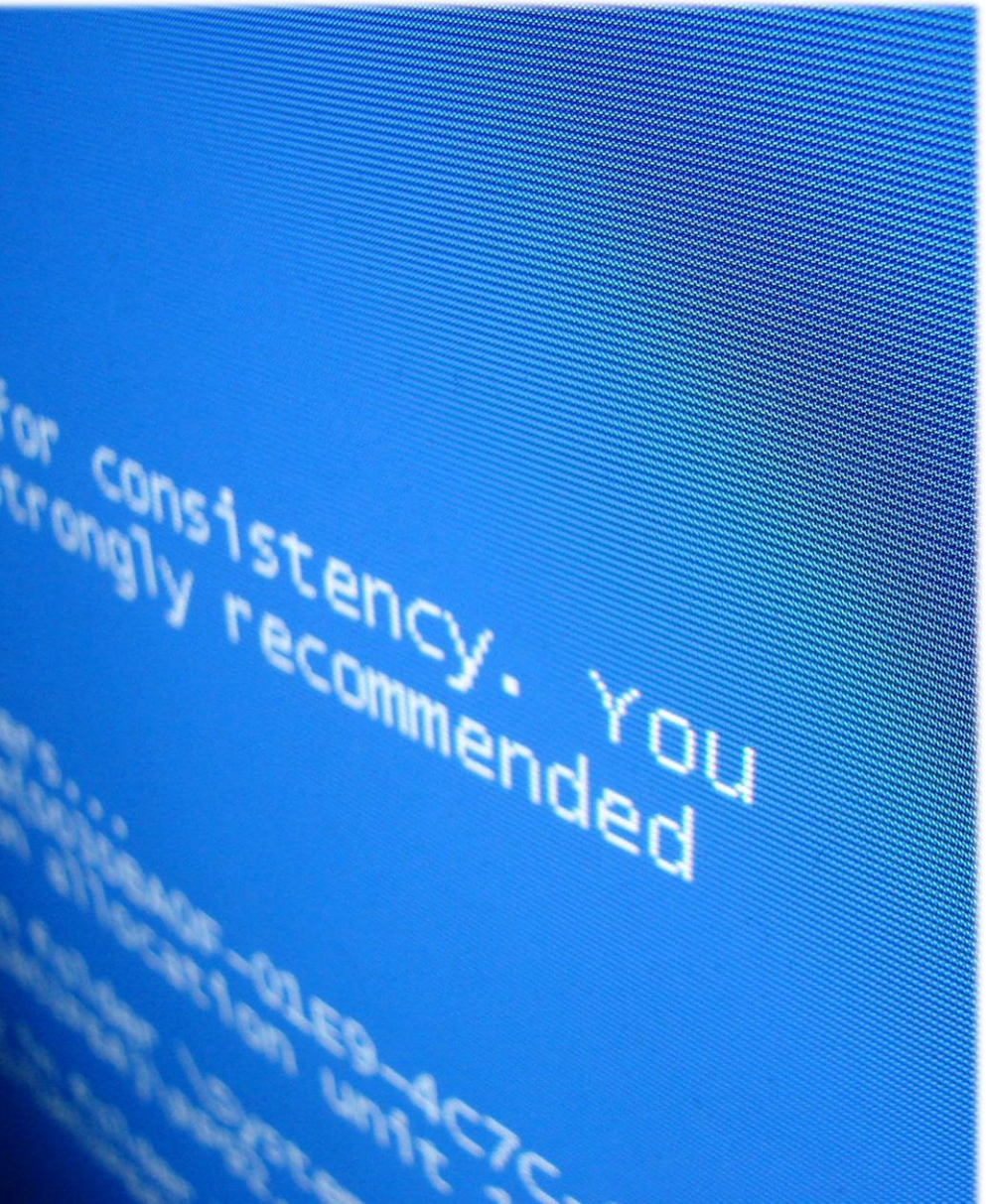


- Passive collection only
- Minimal legal risk
  - Generally, just reading and collecting information about criminal conduct is not illegal
- BUT
  - Disseminating information can be—more on that later
  - Practice good cybersecurity practices—assume the worst

Intelligence Gathering: Posing Questions

- Active engagement, but only in the form of posted questions
- Heightened risk of investigation
  - Just asking questions is not illegal
- BUT
  - You are indistinguishable from an actual criminal seeking assistance
  - Establish a relationship with your local FBI and U.S. Secret Service field office
  - Have organizational policies and procedures in place to establish you true intent
  - Be particularly cautious if you're a solo practitioner

Intelligence Gathering: Exchanging Info



- Actively exchanging information
- Heightened risk of prosecution
  - Beware of providing any assistance
    - "Aiding and abetting" is a crime
    - So is agreeing to commit a crime, even if the crime is never committed and you don't personally take any action
- Provide no legitimate, useful information
- Establish "rules of engagement" or a "compliance program"
- Promptly report any ongoing or impending crime to the authorities

Intelligence Gathering: Criminal Liability*

- Common violations involving furnishing assistance—
  - Aiding and Abetting a Federal Offense (18 U.S.C. § 2)
  - Computer Fraud and Abuse Act (18 U.S.C. § 1030(a))
  - Access Device Fraud (18 U.S.C. § 1029)
  - Fraud in Connection with Identification Documents, Authentication Features, and Information (18 U.S.C. § 1028)
  - Wire Fraud (18 U.S.C. § 1343)

- Potential violations involving agreeing to commit a crime—
  - Federal conspiracy (18 U.S.C. § 371)
  - Conspiracy to violate CFAA (18 U.S.C. § 1030(b))

* Not an exhaustive list

RSAConference2020

Human Directed Active Defense:

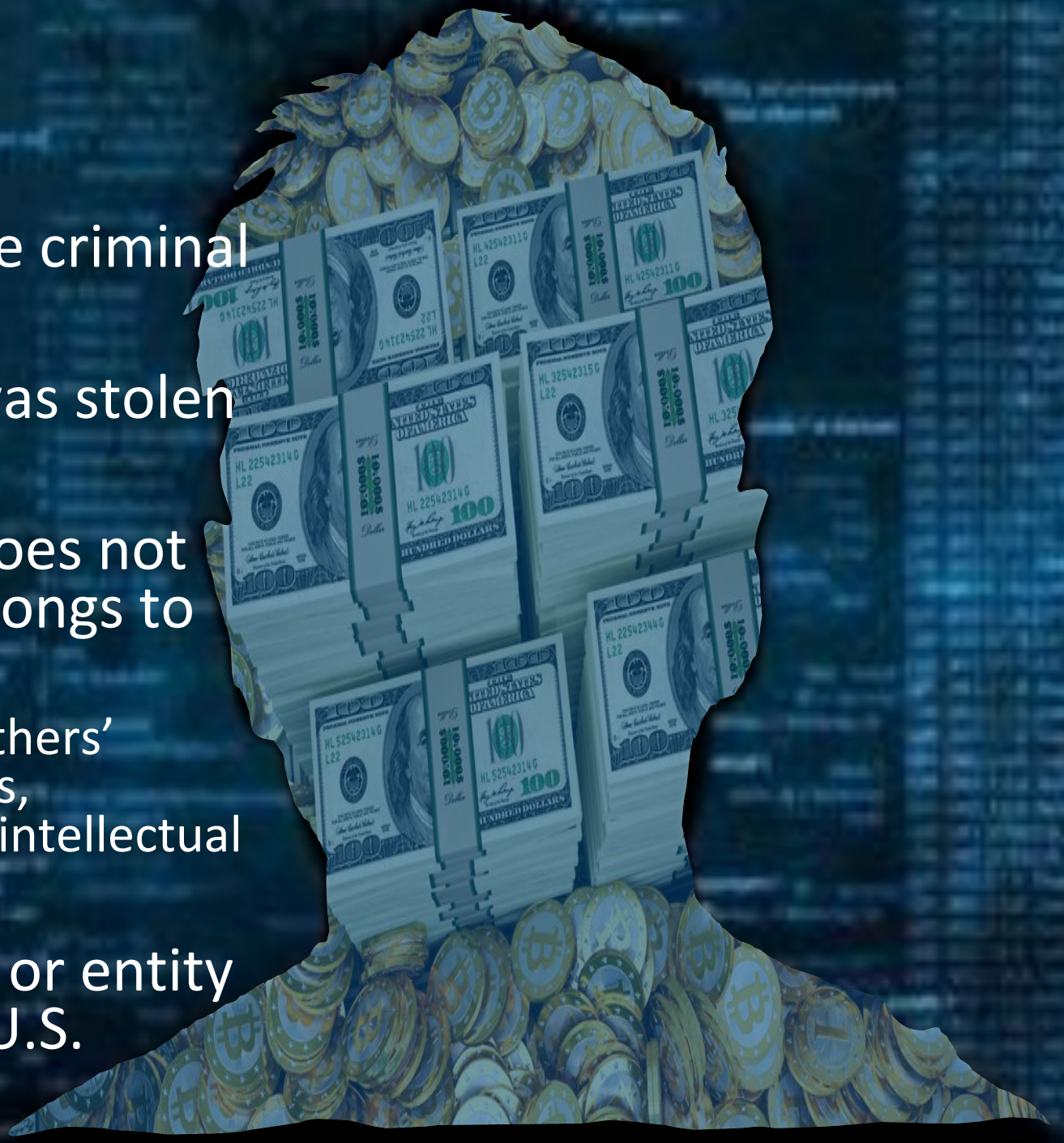
Re-Acquiring Stolen Data and Buying Malware & Security Vulnerabilities

A few words about “TRUST”

U.S. Department of Justice
Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division

Scenario Assumptions

- The purchaser does not have criminal intent
- The data being purchased was stolen from the purchaser
- The data being purchased does not include information that belongs to others
  - In particular, avoid obtaining others' passwords, credit card numbers, authentication information, or intellectual property
- The seller isn't an individual or entity subject to sanctions by the U.S. Government



Reacquiring Stolen Data

- Purchasing your own stolen property is generally not illegal
- BUT legal issues arise –
  - If other parties' information is commingled with yours
  - If you pay an individual or entity that has been designated a "terrorist organization" or as individual or entity for which the Treasury Department has specially designated

U.S. Department of Justice
Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division

Reacquiring Stolen Data: Criminal Liability*

- Potential violations if you possess others' stolen data,—
  - Fraud in Connection with Identification Documents, Authentication Features, and Information (18 U.S.C. § 1028)
  - Access Device Fraud (18 U.S.C. § 1029)
  - Theft of Trade Secrets (18 U.S.C. § 1832)
- Potential violations if you pay a sanctioned entity
  - International Emergency Economic Powers Act (18 U.S.C. § 1705)
  - Material Support to Terrorism Statute (18 U.S.C. § 2339B)

* Not an exhaustive list

Buying Malware/Vulnerabilities

- Merely purchasing malware or vulnerabilities generally is not illegal
- Except –
  - It is illegal to possesses or sells software knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of electronic communications, and
  - that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce (18 U.S.C. § 2512)

U.S. Department of Justice
Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division

How You Should Use DOJ's Guidance

- By next week:
  - Download and read the guidance, available on DOJ Cybersecurity Unit web page (web search for "DOJ Cybersecurity Unit" will get you there)
- Within three months :
  - Assess, with assistance of your organization's legal team, whether your current rules of engagement are consistent with the guidance. They should—
    - Provide operators with direction and red lines for engagement with criminals
    - Cover cybersecurity measures necessary to implement before beginning engagement
    - Identify where in the organization to get legal counsel if questions arise
  - IF YOU DON'T HAVE RULES OF ENGAGEMENT, DEVELOP THEM!
- Within six months:
  - Finalize rules of engagement that are consistent with DOJ's guidance
  - Identify and establish a relationship with local federal law enforcement, possibly through your local FBI Cyber Task Force or Infragard Chapter or U.S. Secret Service Electronic Crimes Task Force

Questions?

U.S. Department of Justice
Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division