Lillian Ablon
Information Scientist
RAND Corporation
@lilyablon

Jay Healey
Senior Research Scholar
Columbia, SIPA
@Jason_Healey

Trey Herr
Fellow
Harvard Kennedy School
Trey_herr@hks.harvard.edu

Katie Moussouris
CEO
Luta Security
@k8em0

Kim Zetter
Journalist &
Author
@KimZetter

Zero Days, Thousands of Nights

The life and times of zero-day vulnerabilities and their exploits

Lillian Ablon

✉ lablon@rand.org

🐦 @lilyablon

RAND
CORPORATION

black hat
USA 2017
JULY 22-27
MANDALAY BAY

- Publicly available research on zero-day vulnerabilities and their exploits is sparse
- Common questions include:
  - **Life Status**: Is a zero-day vulnerability known by others?
  - **Longevity**: How long will a zero-day vulnerability remain undiscovered and undisclosed to the public?
  - **Collision Rate**: What is the percentage of vulnerabilities independently discovered and disclosed in a given time period?
- Answers can help inform decision makers regarding zero-days
- Our research provides empirical analysis of zero-day vulnerabilities and their exploits

Overview of our data

207

Vulnerabilities and their exploits

14

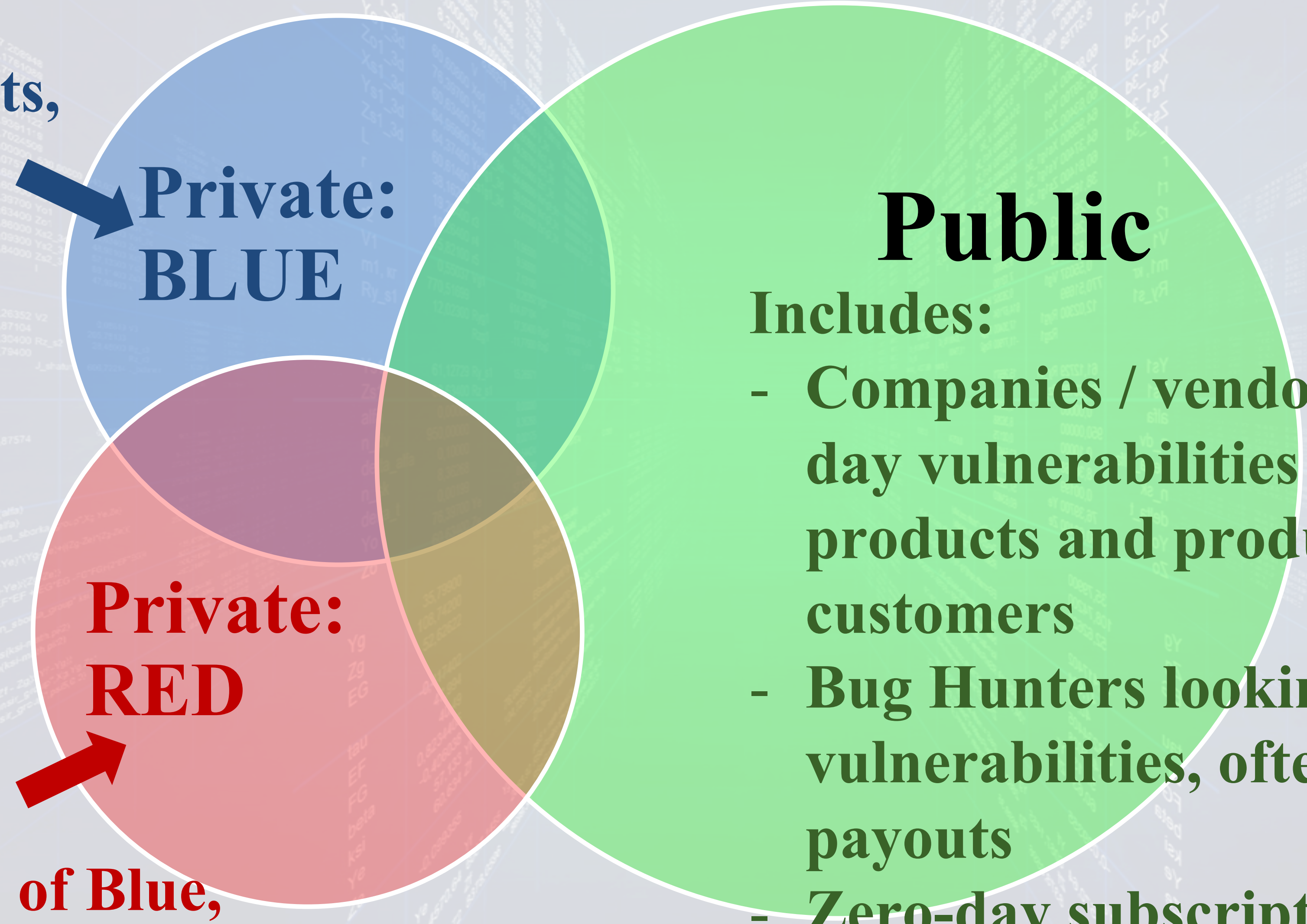
Year span (2002-2016)

BUSBY

Private research group, proxy for a nation-state

Data consists of information about vulnerability class, source code type, exploit class type, vendor, product, exploit developer, and various dates (vulnerability discovery, exploit developed)

Various groups search for vulnerabilities



Governments, defense contractors

Private: BLUE

Private: RED

Adversaries of Blue, Malicious Actors

Public

Includes:

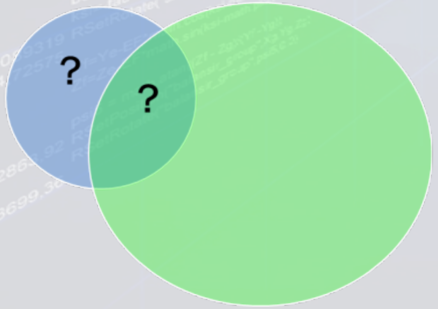
- Companies / vendors looking for zero-day vulnerabilities in their own products and products of their customers
- Bug Hunters looking for zero-day vulnerabilities, often for bug bounty payouts
- Zero-day subscription feed businesses

Key findings in public/private overlap

Life Status

7+ Categories

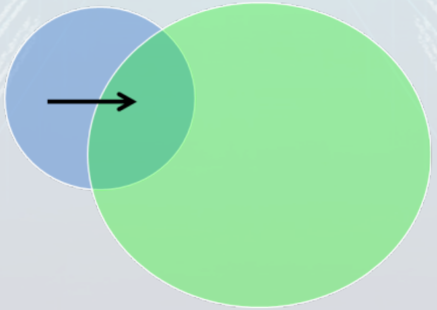
Labeling a zero-day vulnerability as either alive or dead can be misleading and too simplistic



Longevity

6.9 years

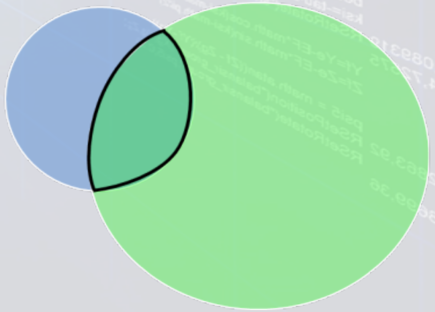
Zero-day vulnerabilities and their exploits have a rather long average life expectancy



Collision Rate

5.7% per year

Time interval examined can significantly change the percentage for likelihood of independent rediscovery



Report freely available at: http://www.rand.org/pubs/research_reports/RR1751.html

Our findings can help inform retention v. disclosure discussions

Pro **retention**

- Long average lifetimes and relatively low collision rates may indicate that:

1. vulnerabilities are dense
    - The level of protection from disclosing a vulnerability may be modest
2. vulnerabilities are hard to find
    - There is a small probability of re-discovery by others

Pro **disclosure**

- Collision rates for zero-day vulnerabilities are non-zero
- A non-zero probability (no matter how small) that someone else will find the same zero-day vulnerability may be too risky

Report freely available at: http://www.rand.org/pubs/research_reports/RR1751.html

Taking Stock: Estimating Vulnerability Rediscovery

TREY HERR, BRUCE SCHNEIER, AND CHRISTOPHER MORRIS

Trey_herr@hks.harvard.edu

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

Dataset

Rediscovery – multiple parties discover the same vulnerability

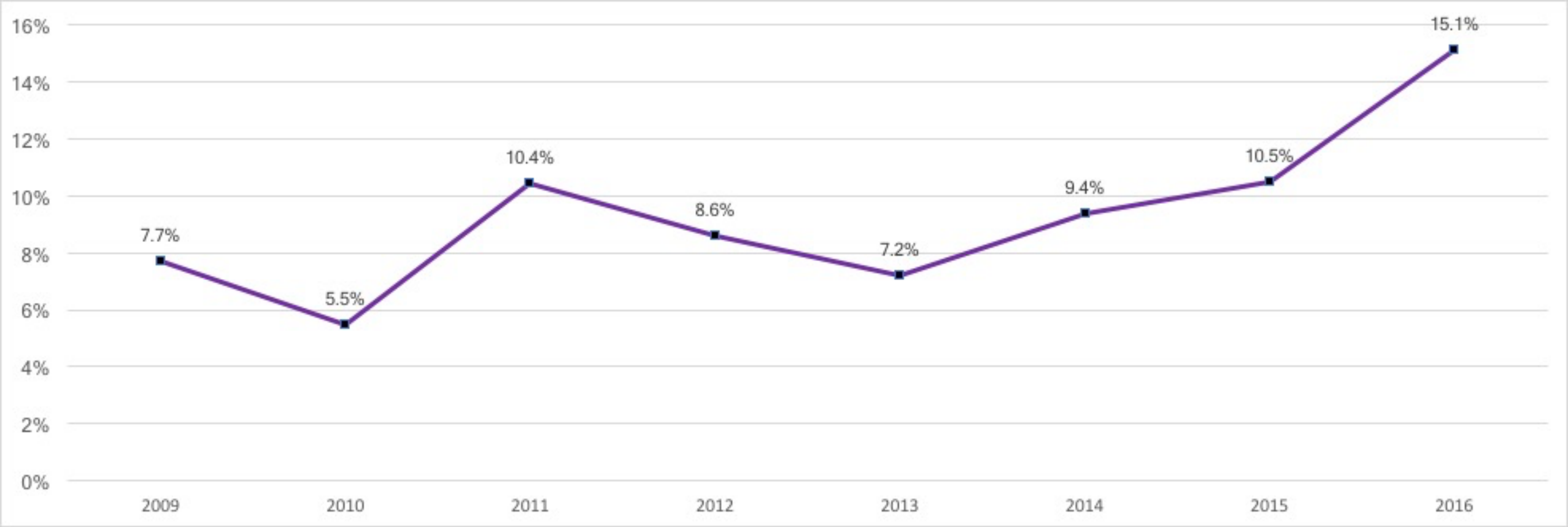
Data

Examined Software	Date Range	Total Population	Sample Vulnerabilities	Sample Duplicates	Rediscovery Rate
Google—Chrome	2009–2016	3354	1739	108	6.2%
Mozilla—Firefox	2012–2016	1112	473	81	17.1%
Google—Android	2015–2016	682	352	77	21.9%
OpenSSL	2014–2016	85	85	2	2.4%
Total	2009–2016	5233	2649	268	10.1%

Results

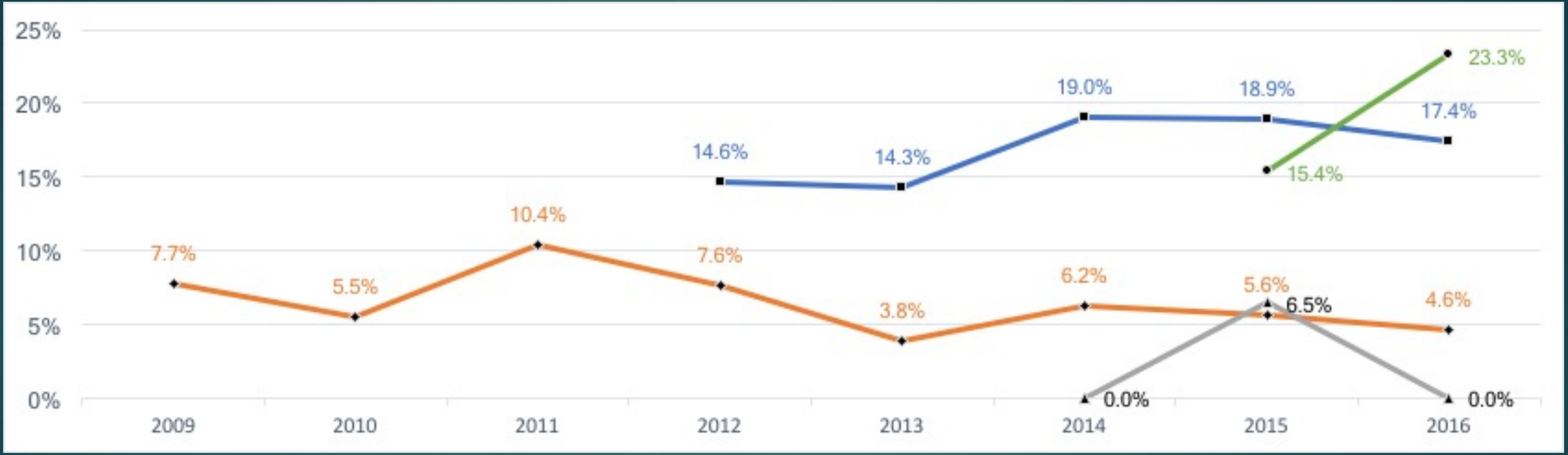
Previous Estimates: 1-6%

Our Estimate: 10-15%



Aggregate Rediscovery Over Time

Rediscovery Rate by Software Type

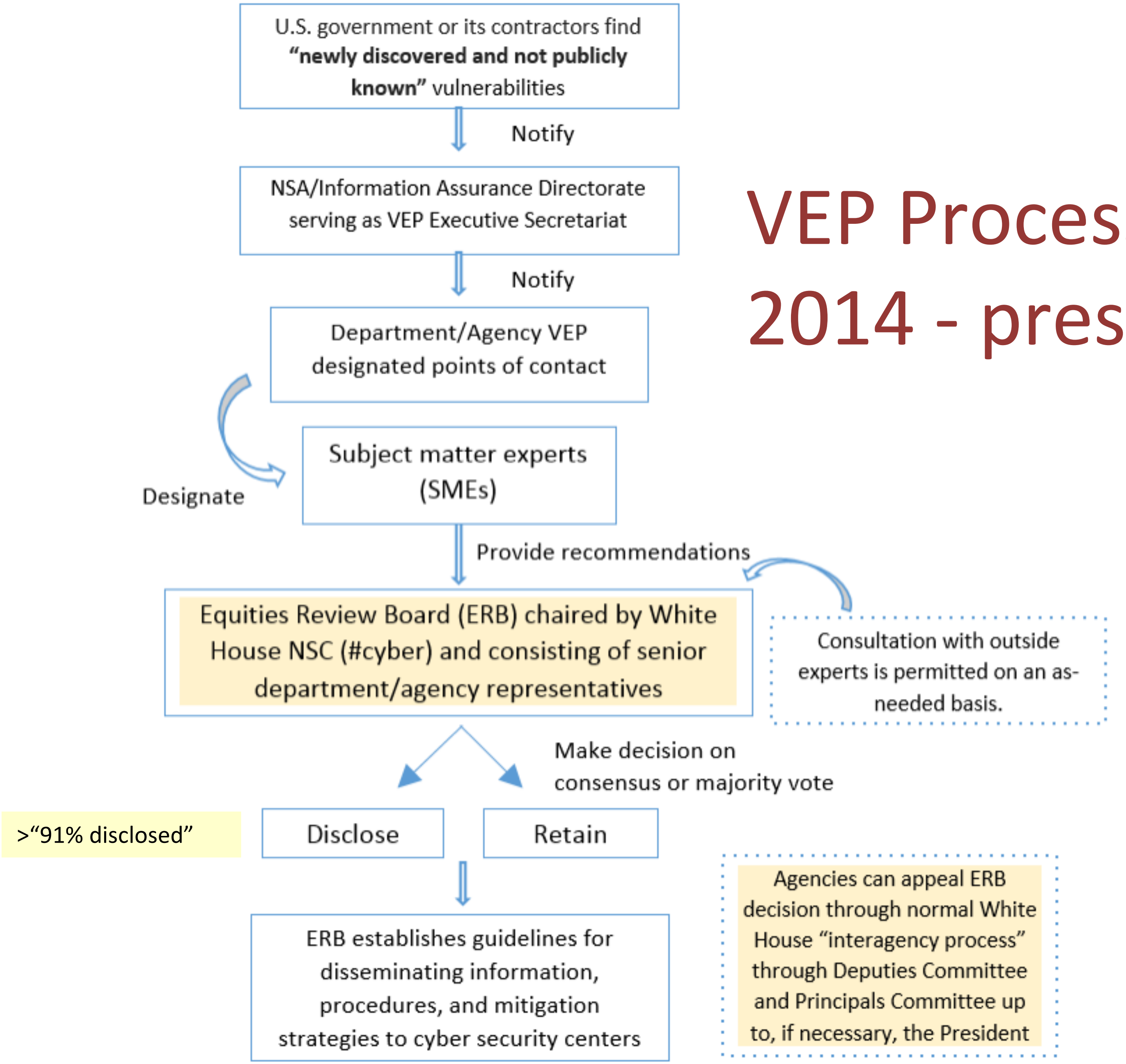


Rediscovery By Software and Year

Outcomes

- More Rediscovery =
  Greater Cost from Non-Disclosure of Software Vulnerabilities
- Product Churn in the Malware Markets
- Patch Prioritization and Informing Bug Bounty Programs

VEP Process 2014 - present



U.S. government or its contractors find **“newly discovered and not publicly known”** vulnerabilities

Notify

NSA/Information Assurance Directorate serving as VEP Executive Secretariat

Notify

Department/Agency VEP designated points of contact

Designate

Subject matter experts (SMEs)

Provide recommendations

Equities Review Board (ERB) chaired by White House NSC (#cyber) and consisting of senior department/agency representatives

Consultation with outside experts is permitted on an as-needed basis.

Make decision on consensus or majority vote

>“91% disclosed”

Disclose

Retain

ERB establishes guidelines for disseminating information, procedures, and mitigation strategies to cyber security centers

Agencies can appeal ERB decision through normal White House “interagency process” through Deputies Committee and Principals Committee up to, if necessary, the President

Lillian Ablon
Information Scientist
RAND Corporation
@lilyablon

Jay Healey
Senior Research Scholar
Columbia, SIPA
@Jason_Healey

Trey Herr
Fellow
Harvard Kennedy School
Trey_herr@hks.harvard.edu

Katie Moussouris
CEO
Luta Security
@k8em0

Kim Zetter
Journalist & Author
@KimZetter