Message in a Bottle: Finding Hope in a Sea of Security Breach Data

DAVI OTTENHEIMER

FLYINGPENGUIN

Session ID: DAS-302

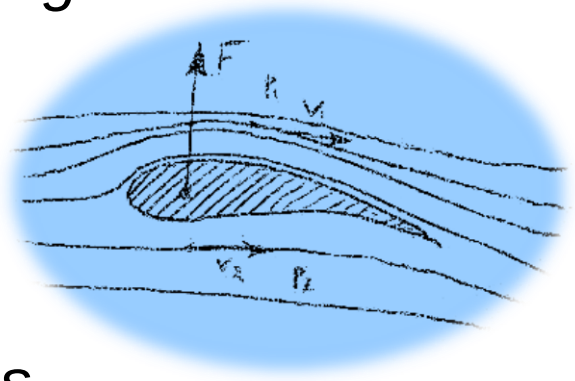
Session Classification: Intermediate

Introduction

INTRODUCTION

flying \fly"ing\, a. [From fly, v. i.]

moving with, or as with, wings; moving lightly or rapidly; intended for rapid movement



penguin \pen"guin\, n.

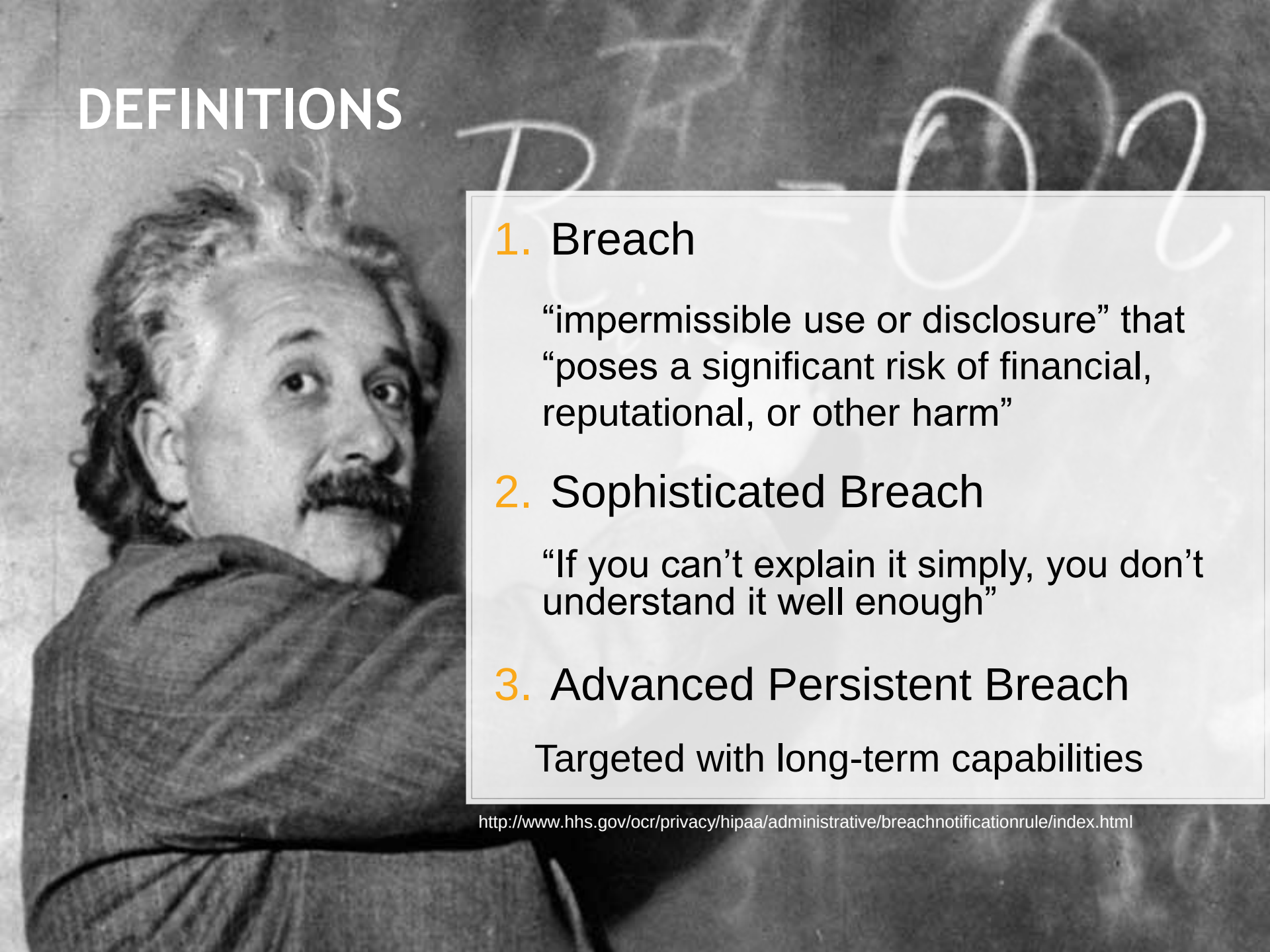
short-legged flightless birds of cold southern especially Antarctic regions having webbed feet and wings modified for water

AGENDA

- Background and Data
- Analysis: Who, What and How
- What it all Means

Background and Data

DEFINITIONS



1. Breach

   "impermissible use or disclosure" that "poses a significant risk of financial, reputational, or other harm"

2. Sophisticated Breach

   "If you can't explain it simply, you don't understand it well enough"

3. Advanced Persistent Breach

   Targeted with long-term capabilities

http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html

DATA

“It's a fundamental principle of copyright law that facts are not copyrightable…”

- Electronic Frontier Foundation, 2012

https://www.eff.org/press/releases/eff-wins-protection-time-zone-database

SOURCES

- Trustwave
- Verizon
- Trend Micro
- Sophos
- McAfee
- Dell SecureWorks
- AlienVault
- Secunia
- Ponemon
- US States (NCSL)
- privacyrights.org
- Identity Theft Resource Center
- **HHS.gov**

"As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals."

http://www.ncsl.org/issues-research/telecom/security-breach-notification-laws.aspx,
http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html

TRUSTWAVE SPIDERLABS

WP Global Security Report 2012

- 300 Investigations
- 18 Countries
- 20% unknown method of entry
- 33% unknown origin

VERIZON

2011 Data Breach Investigations Report

- 834 Cases (40% Hospitality, 25% Retail, 22% FSvc)
- 33,000 Attack Steps
- 54 Intersections of Agent/Action
- Threat sources
  - 3% China (50% if you count last hop)
  - 65% Europe-East
  - 19% Americas-North
  - 12% Unknown

TREND MICRO

A Look Back at 2011: Information is Currency

- "Year of Data Breaches"
  - Fewer vulns, more complex attacks
    - CVE-2011-3402 – CVSS 9.3 – TrueType win32k.sys
    - CVE-2011-3544 – CVSS 10.0 – JRE
    - CVE-2011-3414 – CVSS 7.8 – ASP.NET HashTable
  - "unenlightened users will make a mistake…no matter what social network you drop them into"
- 3.5 new threats created every second
- Top spam countries: India 18%, Russia 15%

The "Lurid" Downloader (Enfal from 2002)

SOPHOS

Security Threat Report 2012

- 80% of infected sites legitimate
- 67% of detections are redirections
- Mobile, Social Networks, Removable Media

  "Security basics like patching [Conficker] and password management will remain a significant challenge"
- Top spam countries: US 12%, India 8%
- Top spam continents: Asia 45%, Europe 26%
- PCs most attacked: Chile, China, South Korea

MCAFEE

McAfee Threats Report: Fourth Quarter 2011

- 40 Breaches reported in Q4
- Spam and malware in *decline*
- Mobile malware rising
- Malicious URLs up 8x in 2011
- 73% of malicious content hosted in the US

VISUAL EXPLANATIONS

- by Edward R. Tufte
- *Images and Quantities, Evidence and Narrative*

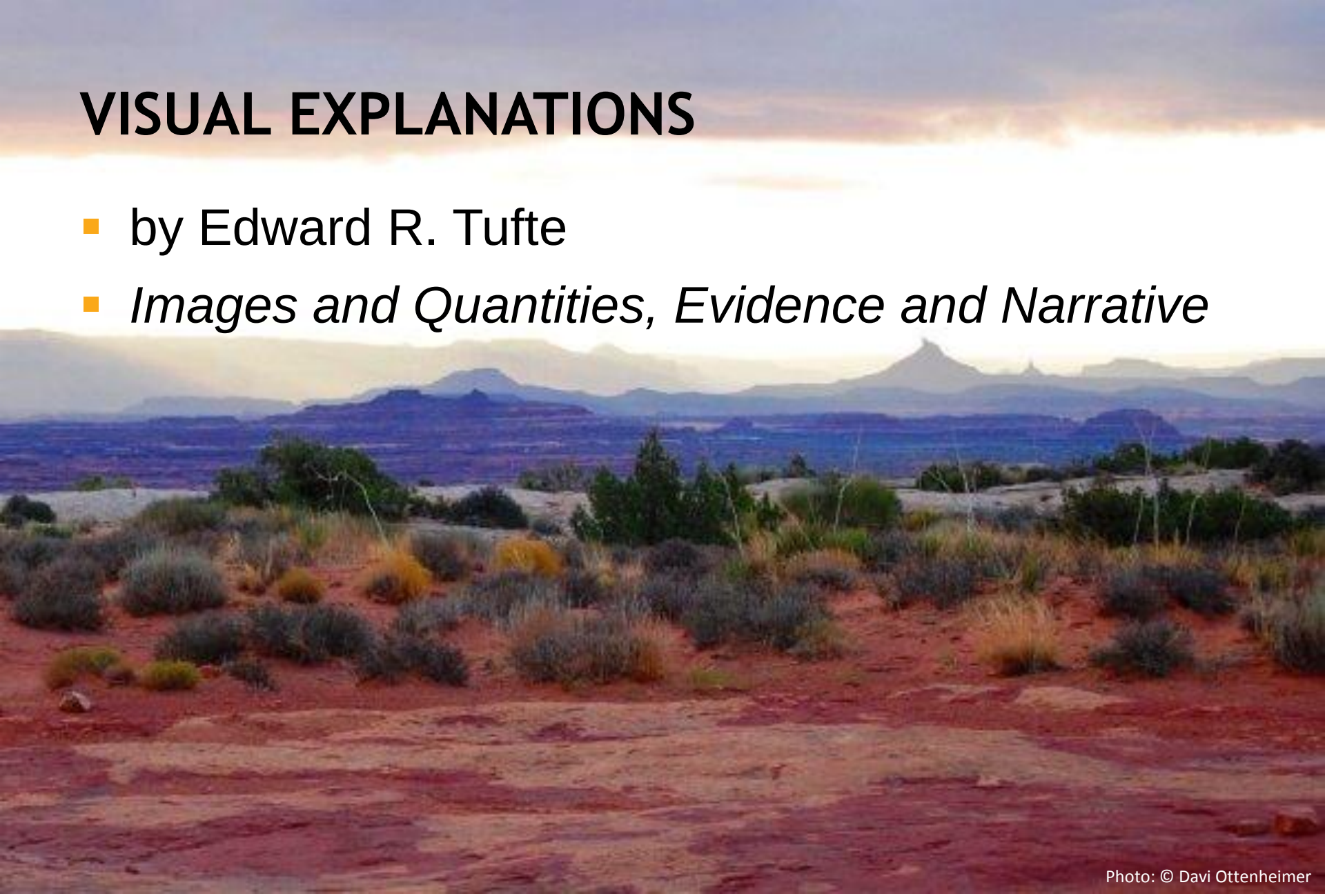


Photo: © Davi Ottenheimer

HEALTH RISKS: CHOLERA EPIDEMIC

Epidemiology to Public Policy

- 616 Deaths: London, August to September 1854
- Dr. John Snow, Investigates
  - 1831-1832 first studied cholera
  - 1848-1849 develops water “poison” theory

    Book: *On the mode of communication of cholera*
  - 1854 “Ghost map” highlights Broad Street pump
- Convinces Parish Council to remove handle

GHOST MAP

- = Deaths
- = Pump

http://www.udel.edu/johnmack/frec480/cholera/cholera2.html

HEALTHCARE RISKS BY EXPENSE

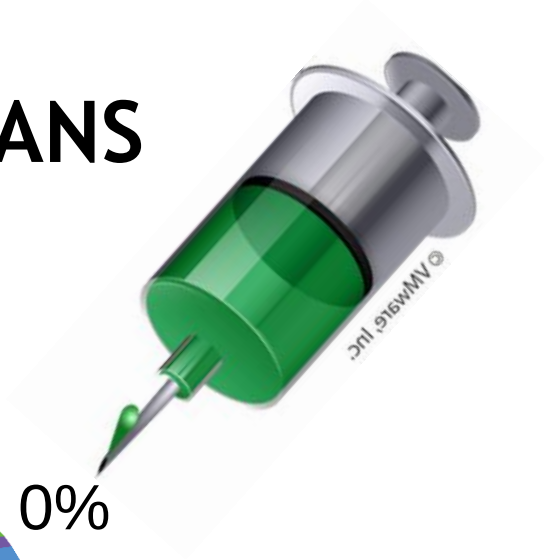
"New study shows **data breaches** up and **costing healthcare industry billions of dollars a year**, with employees, mobile devices the weakest link."

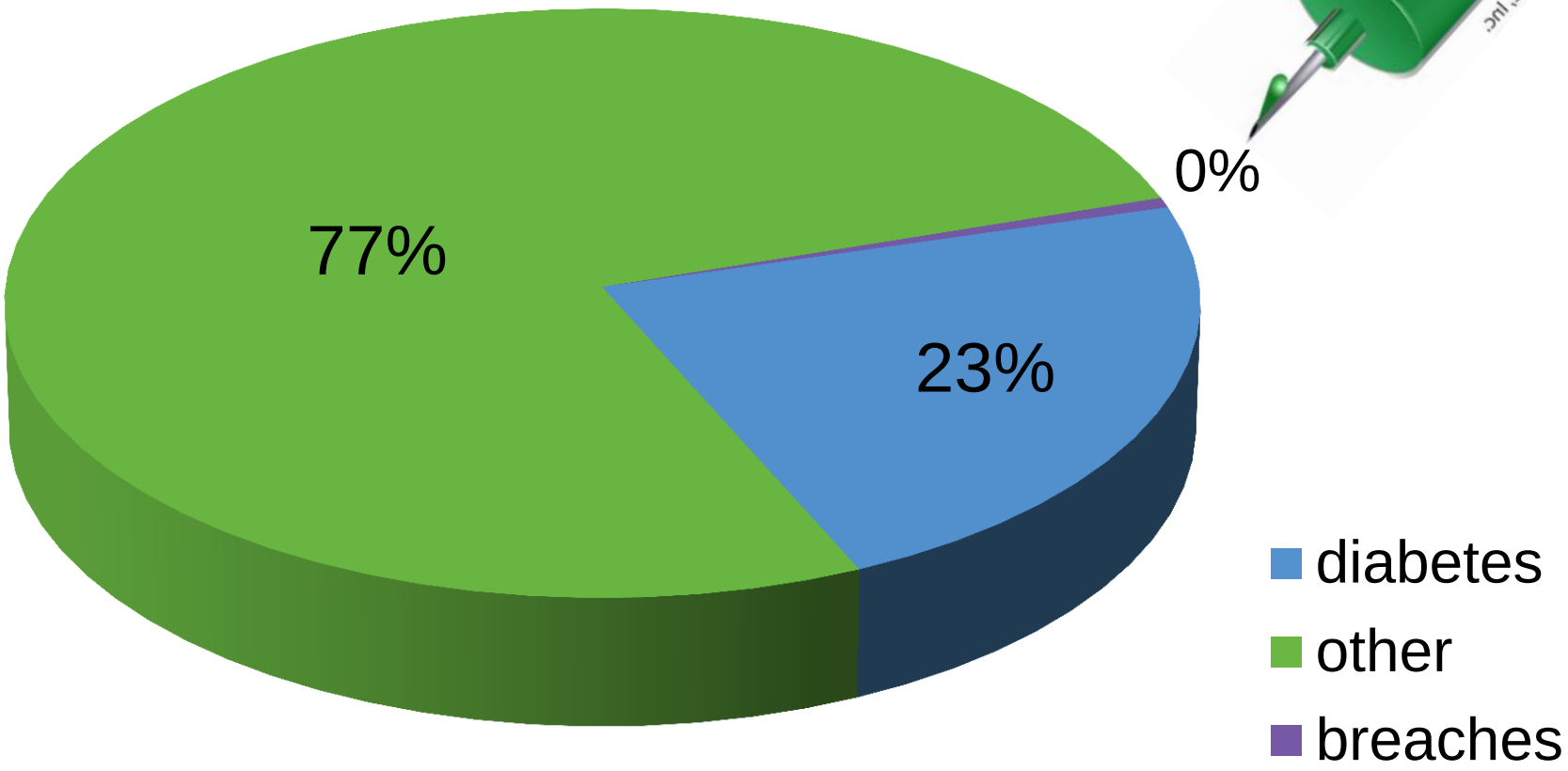
"…according to a report released last week from the Agency for Healthcare Research and Quality (AHRQ), **[diabetes is] costing Americans $83 billion a year** in hospital fees — 23 percent of total hospital spending."

http://www.darkreading.com/insider-threat/167801100/security/attacks-breaches/232200606/healthcare-data-in-critical-condition.html

http://www.thefiscaltimes.com/Articles/2010/08/19/The-Cost-of-Diabetes.aspx

HEALTHCARE COSTS TO AMERICANS





COMPETITION RISKS (INDYCAR)

- 1911 Aerodynamics
- 1911 Rear-view mirror
- 1921 Four-wheel hydraulic brakes
- 1924 Front-wheel drive
- 1932 All-wheel drive
- 1952 Turbochargers
- 1956 Seat-belts…

https://truthaboutmornings.wordpress.com/2011/12/02/things-your-rearview-mirror-doesnt-show-you/
http://www.msnbc.msn.com/id/43074652/ns/business-autos/t/top-indycar-technologies/

SEATBELTS – BRIEF HISTORY

- 1885 - Patent (US)
- 1930s - Physicians Encourage Use
- 1948 - JAMA Article

  Medical Criticism of Modern Automotive Engineering
- 1949 - Optional Issue (Nash)
- 1955 - JAMA Article

  Prevention, the Only Cure for Head Injuries…
- 1958 - Standard Issue (Saab)
- 1970 - Required by Law (Australia)

http://jama.ama-assn.org/content/159/10/981.full.pdf, http://jama.ama-assn.org/content/138/9/627.short

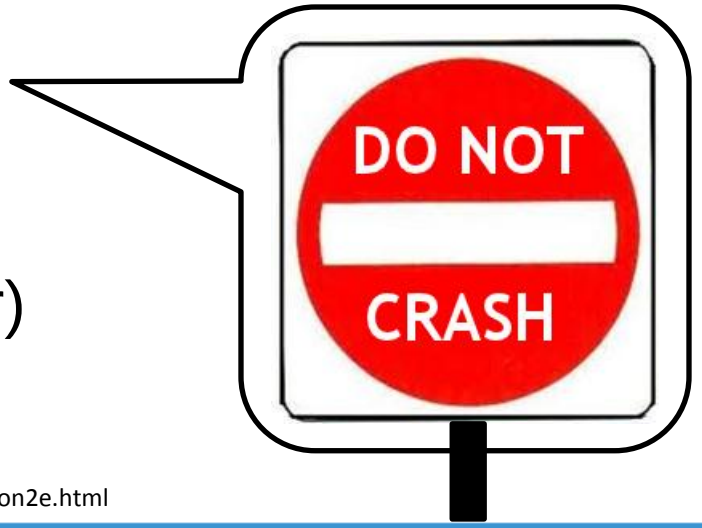
SEATBELTS – BRIEF ANALYSIS

- Reduced risk of injury

> *"Seat belts reduce the risk of being killed or seriously injured in a crash by about 50%"*

- Improved strength at $500/ea reduces injury only 3%
- Better road signage helps 8%
- Airbag helps 10% - 25%

  (297 lbs of structure, 12 yr younger)

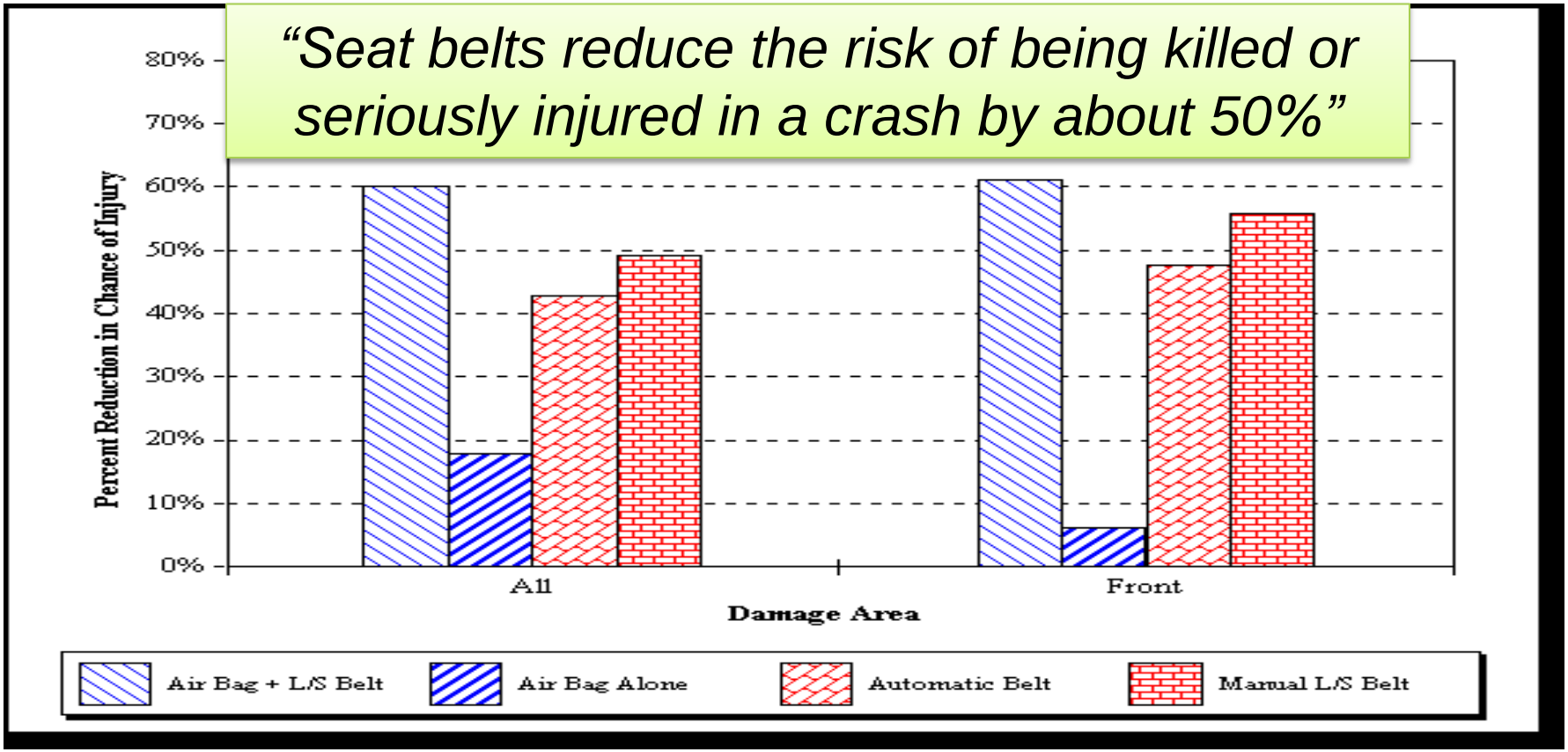


http://www.cdc.gov/Features/VitalSigns/SeatbeltSafety/, http://www.nhtsa.gov/people/injury/airbags/208con2e.html

SEATBELTS – BRIEF ANALYSIS

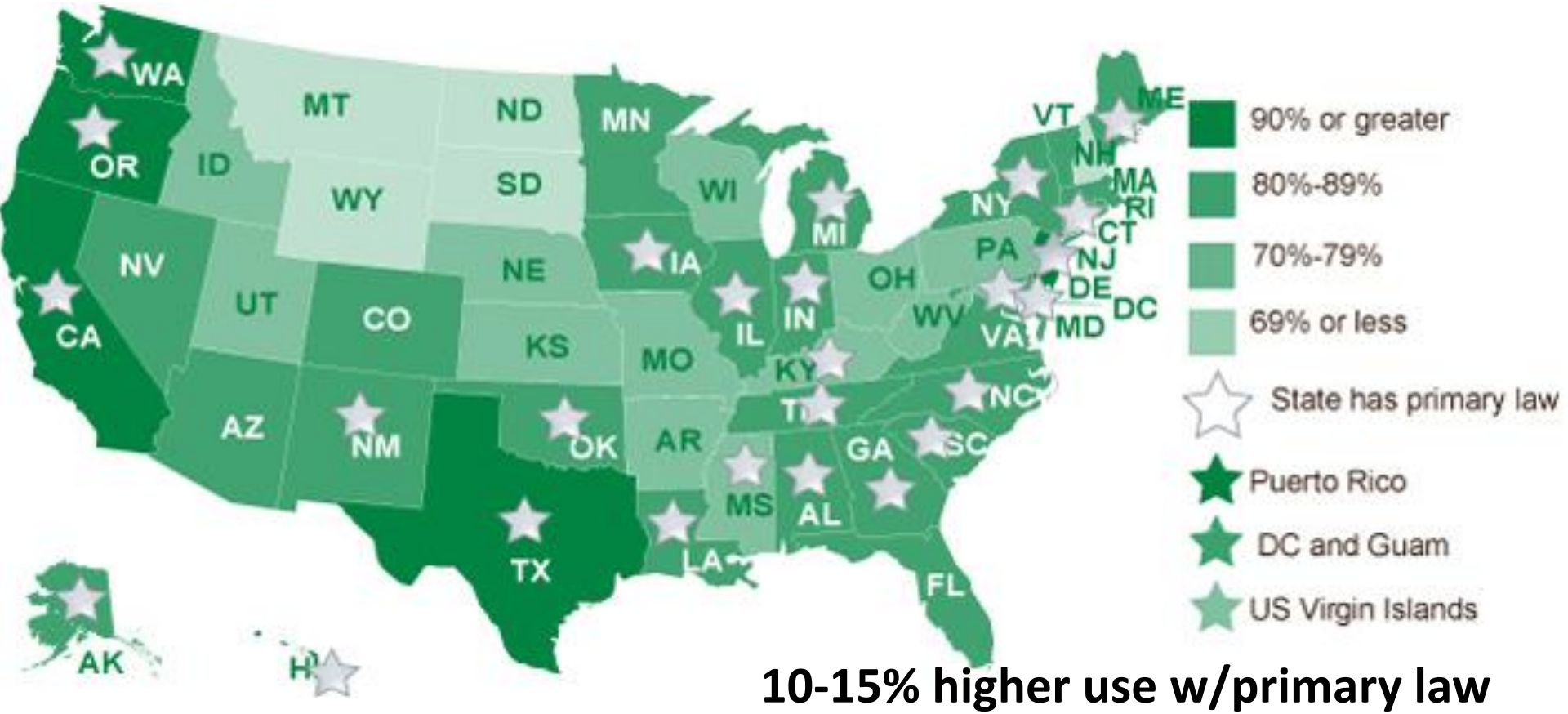
- Reduced risk of injury

"Seat belts reduce the risk of being killed or seriously injured in a crash by about 50%"



http://www.cdc.gov/Features/VitalSigns/SeatbeltSafety/, http://www.nhtsa.gov/people/injury/airbags/208con2e.html

SEATBELTS – BRIEF ANALYSIS



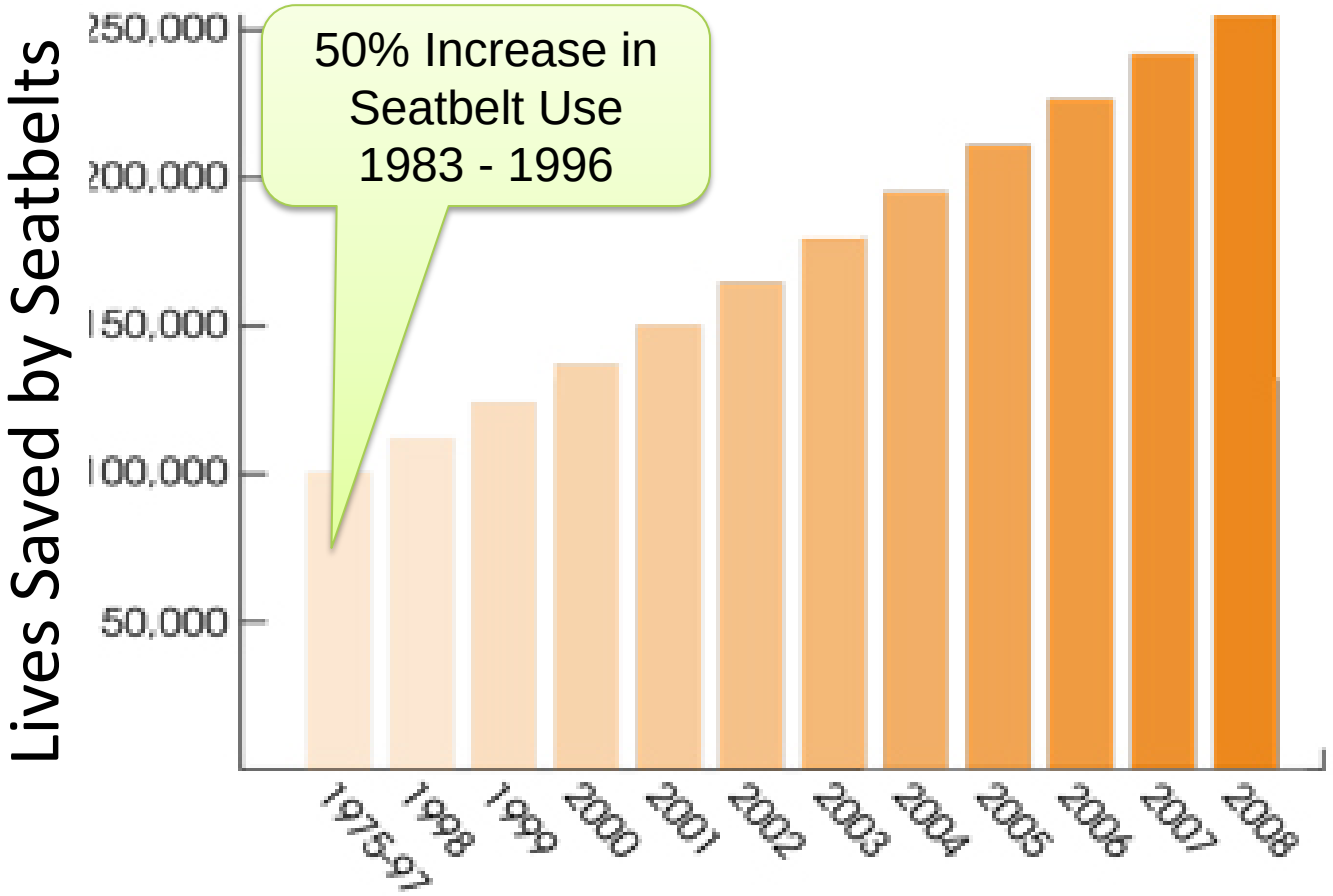
injury rate overall declined 15%

http://www.cdc.gov/vitalsigns/SeatBeltUse/StateInfo.html

10-15% higher use w/primary law

- 2002: 18 states, 53% coverage
- 2008: 26 states, 65% coverage

SEATBELTS – CONCLUSION



http://www.cdc.gov/motorvehiclesafety/seatbeltbrief/, http://www.nhtsa.gov/people/injury/airbags/Archive-04/PresBelt/america_seatbelt.html

…OTE: WHY IS AVIATION SAFER?

"…some young people feel that driving interferes with texting and other electronic communication"

The "root of Afric… …y record"

1. Low investment, crumbling i…
2. Lax national authorities
3. Minimal air-traffic control or regulation
4. *Basic navigational aids*

http://www.fieldtechnologies.com/, http://automotivegpssystems.org/, http://www.ascendworldwide.com/the_wall_street_journal_15-08-07.pdf
U-M Transportation Research Institute: http://www.valkyrieforum.com/bbs/index.php?action=printpage;topic=35767.0

Analysis: Who, What and How

TRUSTWAVE SPIDERLABS

- 78% Food and Beverage Industry + Retail
- 89% Customer Records
- 76% Related to Partners
- 5x Increase External Detection (Law Enforcement)
- 88% of Malware not Detected (12% Effective)
- SQL Injection #1 Attack
- Password1 b/c “satisfies default AD requirement”

VERIZON

- External – 92% of Breaches, 99% of Records
- Internal – 17% of Breaches, 1% of Records
  - 85% end-user
  - 22% finance/accounting
- Partners – 0% (down from 22% in 2010)
- Causes
  - Malware 49%
  - Hacking 50%
  - Physical 29%

(Social Network Attacks just 5% of Social Engineering)

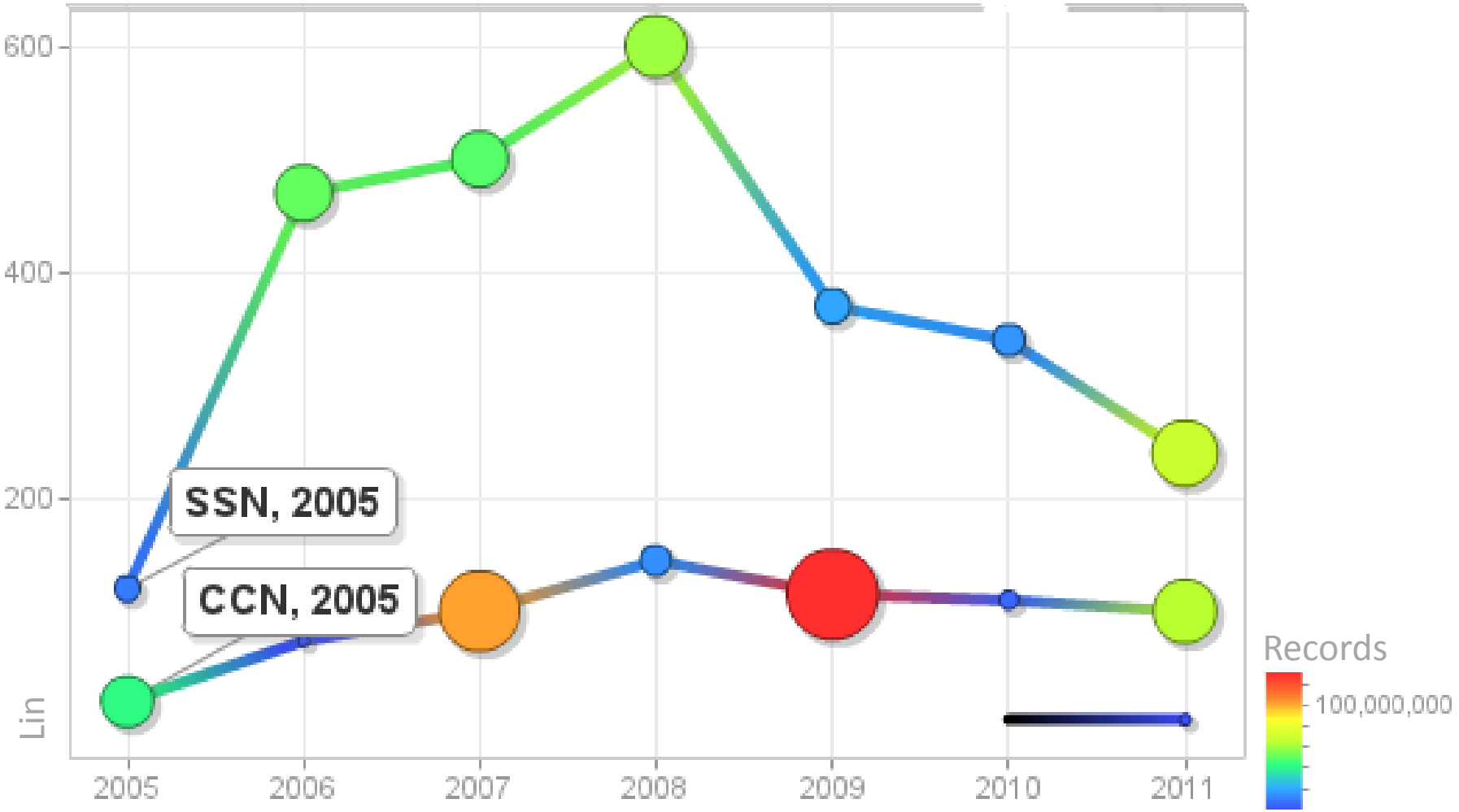
VERIZON

- Risk 60% lower if ***response sub 2 hours***
- No new cat. of attack – ***scan for just 5 ports***
- Where to spend money
  1. Identity (Default or guessable, then weak pwords)
  2. SQL Injection
  3. Monitoring non-critical servers
- 85% Externally notified
- Patch In 5-6 mos, AV 8-9 days = < 10% benefit
- 4.7 steps per attack – ***only need to stop one***

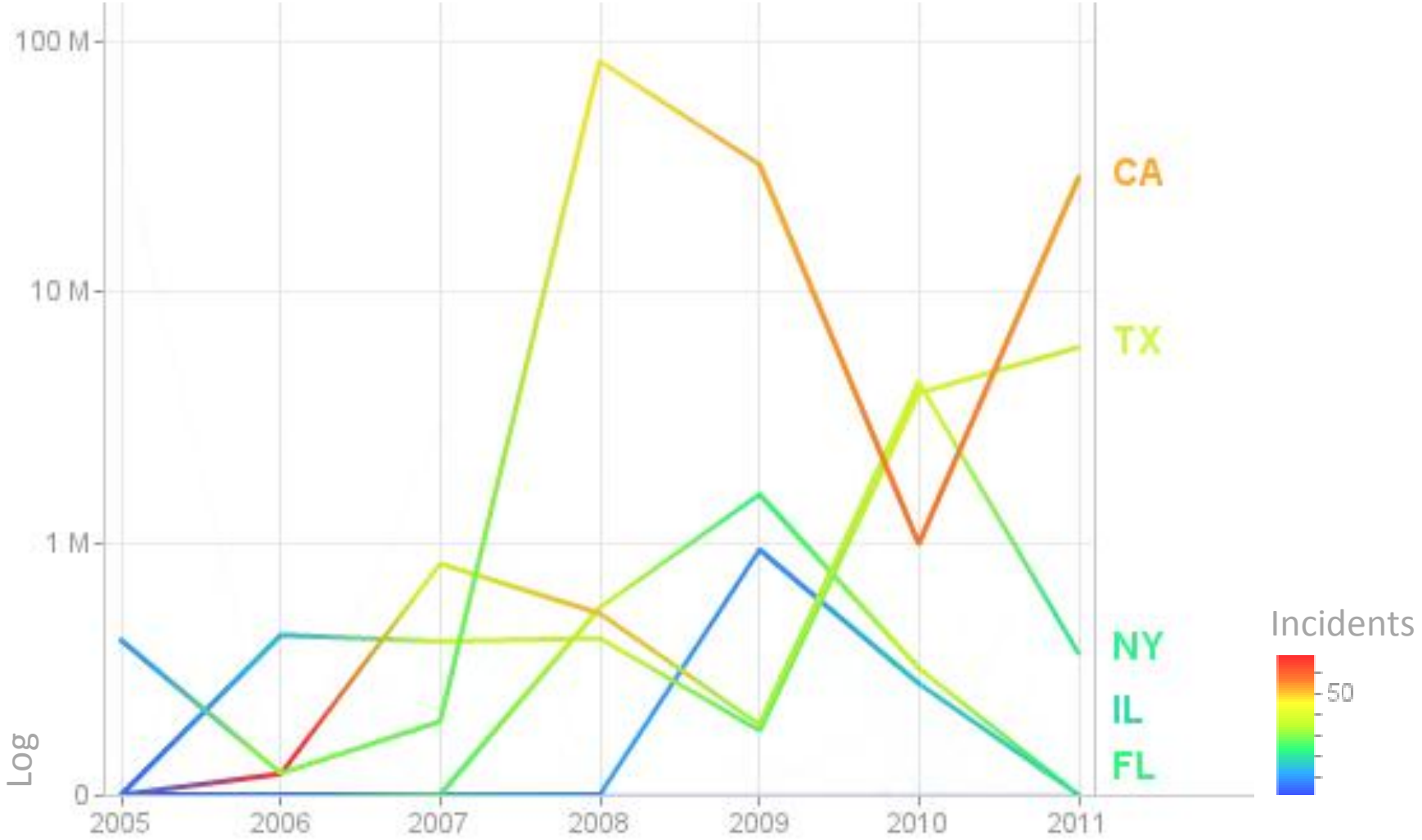
PUTTING IT TOGETHER

1. Perimeter improvements working (keep it up)
2. Attackers focusing on *exceptions*
   - VPNs (Tokens)
   - Apple and Android (BYOD)
   - Unusual Services (Backdoors)
   - Egress ports (80, 443, 25)
   - End-user interface (Social decisions / overrides)
3. Any and every *asset* is a target
4. Source of attacks *mostly* unknown but *social*

SHIFT IN IDENTITY BREACHES?

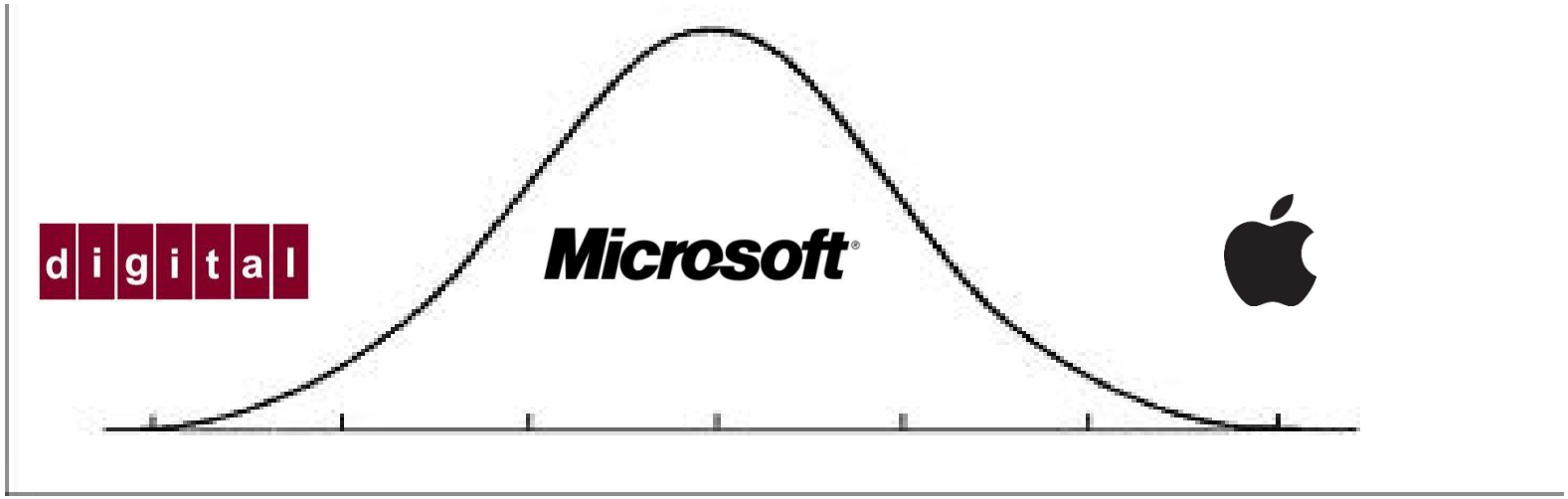


BREACHES IN 5 MOST POPULATED STATES



ATTACK VECTORS

1. Default or Weak Credentials
2. Lack of Input Filtering (Inclusion, Injection)
3. Excessive Services Allowed
4. Fringe Systems (Legacy and New) Unpatched



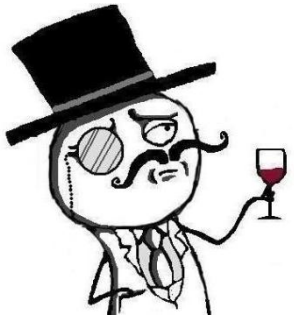
FOUR STEP ATTACK PROCESS

1. Enumerate
   - All vulnerabilities on a system
   - All systems with a vulnerability
2. Access
   - Injection/Incusion/Credentials
   - Load malware
3. Control
   - Dump stored data
   - Dump data in transit
4. Expand and repeat

SAMPLES

1. Anonymous and LulzSec
2. Virtualization
3. Cloud
4. Certificates
5. Tokens
6. “Material”

1. ANONYMOUS AND LULZSEC

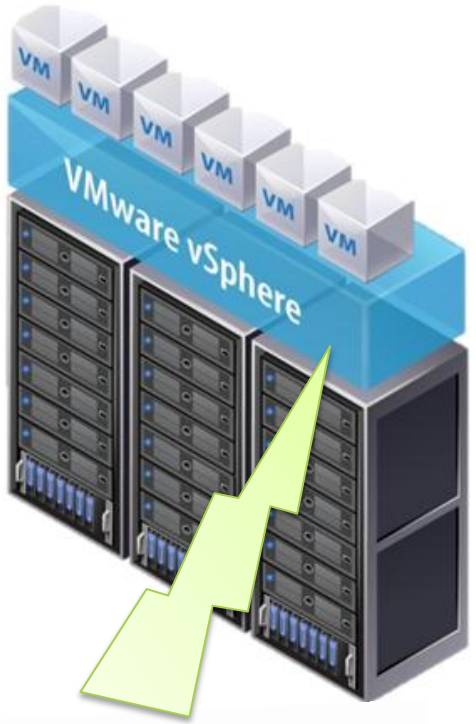


- AT&T: June 2011
  1. Convergys (70,000 staff) hires Moore to call center
  2. Moore granted VPN access
  3. Anonymous post to fileape.com of AT&T property
  4. System of egress narrowed to 19 contractors
  5. Moore used his account to access AT&T servers
  6. Moore used his account to search Google for “uploading files, file hosting, and uploading zip files”
  7. Moore present and working at time of egress

http://www.flyingpenguin.com/?p=13063

2. VIRTUALIZATION

- Shionogi: February 2011
- “Cornish [deleted] the contents of each of 15 ‘virtual hosts’ on Shionogi’s computer network…housed the equivalent of 88 different computer servers.”



http://www.flyingpenguin.com/?p=13259

3. CLOUD

- Epsilon: April 2011
  - 2,000 customers and over 40 bil email a year
  - Info on 250 mil consumers and 22 mil businesses
  - Email addresses and customer names stolen
  - Office of the Information and Privacy Commissioner of Alberta, Canada: “real risk of significant harm”
- Group of email service providers targeted (Silverpop, AWeber Communications) and platform (ReturnPath)?
- Was email sent to employees with malware attachment?

http://www.oipc.ab.ca/Content_Files/Files/News/NR_Epsilon_May_2011.pdf

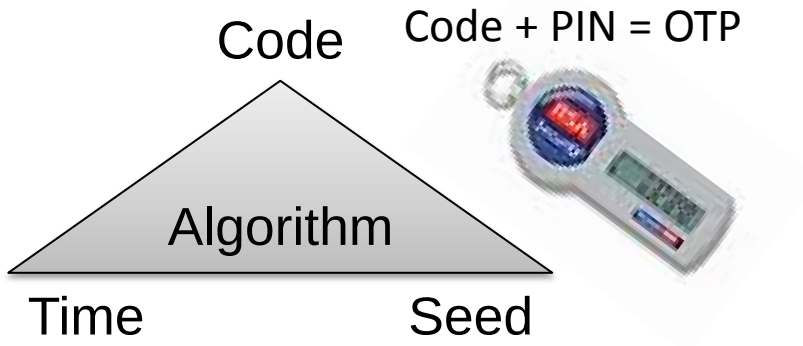
4. CERTIFICATES

- DigiNotar: September 2011
  - Records fail
    - Google certificate serial # not in system records
  - Infrastructure fail
    - Lack of segmentation – all CA servers in one Domain
    - Weak Domain administrator password
    - Missing patches
    - Compromised systems unnoticed (and replicated)
    - Lack of centralized logs
  - Response fail
    - Evidence back to 2009 not noticed or investigated
    - External alert/pressure

https://www.eff.org/observatory

5. TOKENS

- RSA: April 2011
  - Two different phishing email in two days with malware
    2011 Recruitment plan.xls - (CVE-2011-0609) Flash vuln
  - User pulls email from junk folder, executes
  - Back door (RAT) established, “phones home”
  - Attacker searches to expand internal access
  - Data collected on SecurID
  - Attack detected by CIRT
- Sykipot -> ActivClient PIN



http://blogs.rsa.com/rivner/anatomy-of-an-attack/

6. "MATERIAL"

"…material information regarding cybersecurity risks and cyber incidents is required to be disclosed" - SEC

- 2009 RockYou password/email (2011 ruling)

  "…sufficiently alleged a general basis for harm…some ascertainable but unidentified 'value' and/or property right inherent in the PII…"

- 2011 RSA SecurID breach

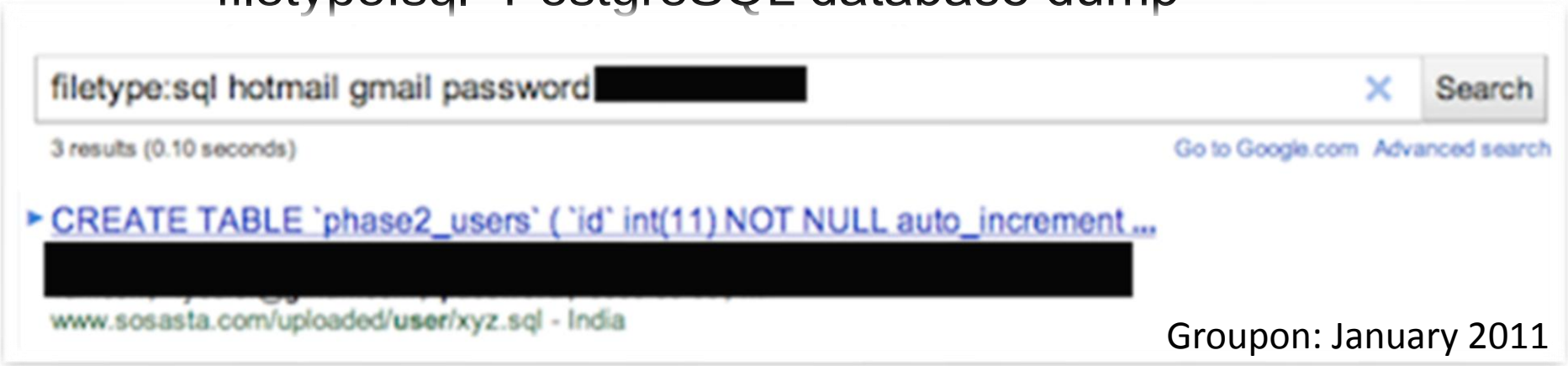
  "In an 8-K filed on March 17, 2011, EMC told investors that the event wouldn't have a material impact on the company or its financial results."

http://www.scribd.com/doc/53080958/Claridge-v-Rockyou-09-6032-PJH-N-D-Cal-Apr-11-2011, http://www.bloomberg.com/news/2012-01-10/sec-push-may-yield-new-disclosures-of-cyber-attacks-on-companies.html, http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

6. “MATERIAL”

Word	Count	Of total
123456	290729	0.8917 %
12345	79076	0.2425 %
123456789	76789	0.2355 %
password	59462	0.1824 %
iloveyou	49952	0.1532 %

- Google dorks
  - inurl:-cfg intext:"enable password"
  - filetype:ini "[FFFTP]” (pass|passwd|password|pwd)
  - filetype:sql “phpmyAdmin SQL Dump” (pass|password|passwd|pwd)
  - filetype:sql “PostgreSQL database dump”



Groupon: January 2011

http://risky.biz/sosasta

WHAT IFs

- Attackers make the same mistakes…
- We use the methodology in reverse
- We use correlative data collection on attackers

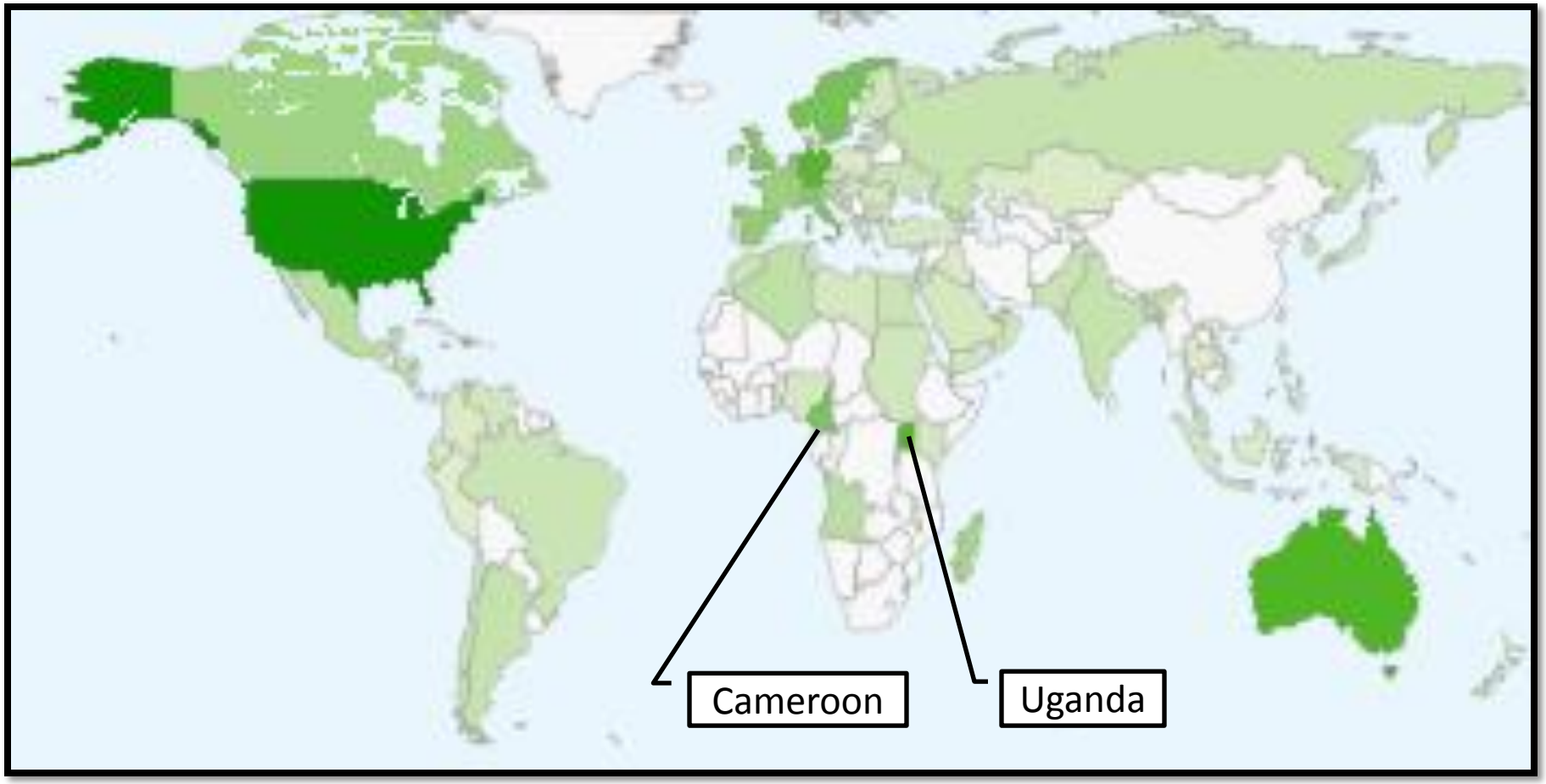
NEW FORMS OF ID? (REPUTATION)

12 million Tweets, 10-12/ 2011

http://www.wired.co.uk/news/archive/2012-01/27/africa-twitter-traffic?utm_source=twitter&utm_medium=socialmedia&utm_campaign=twitterclickthru

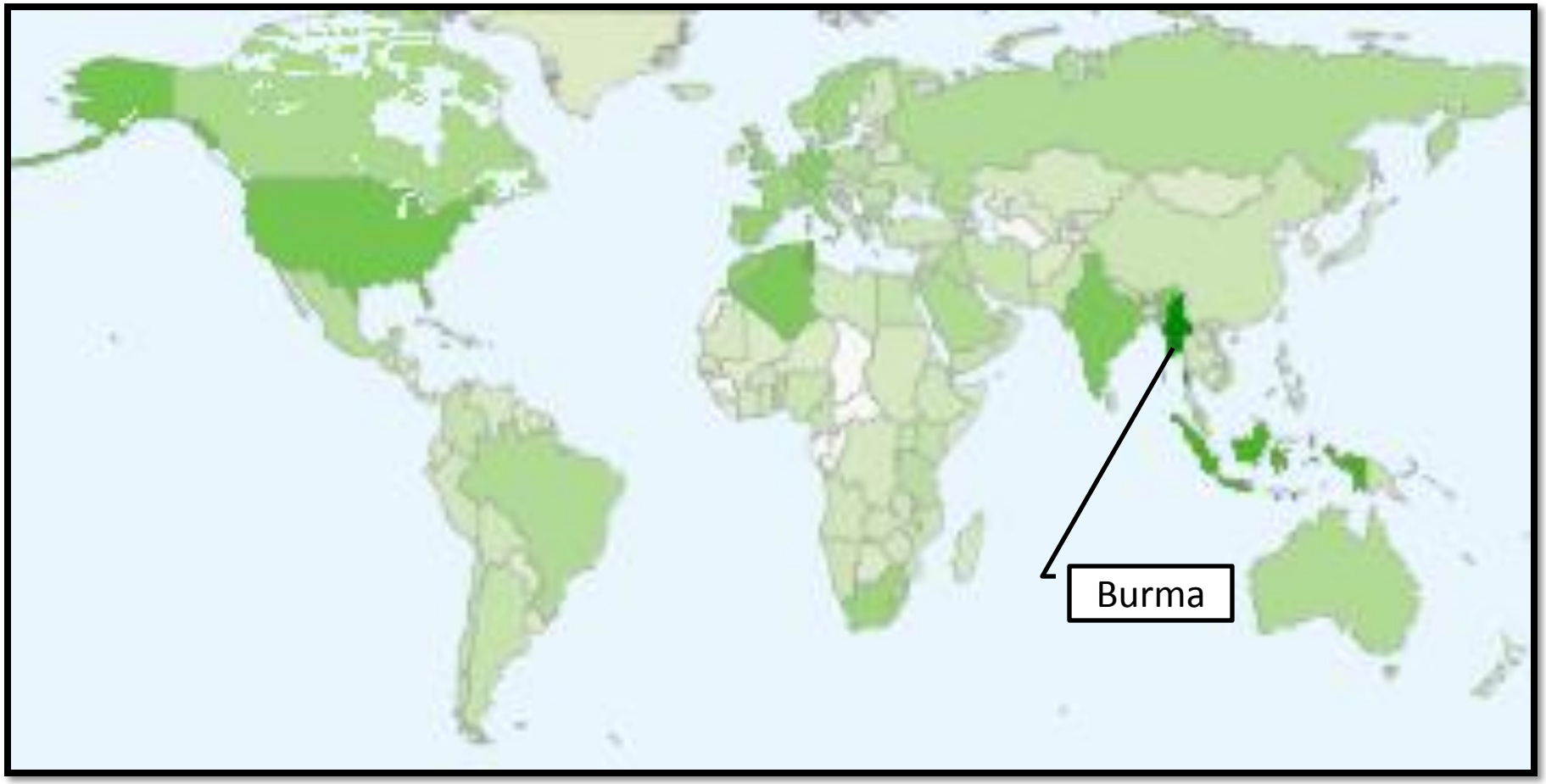
ATTACKER ID?

- Black Hole RAT Tutorial



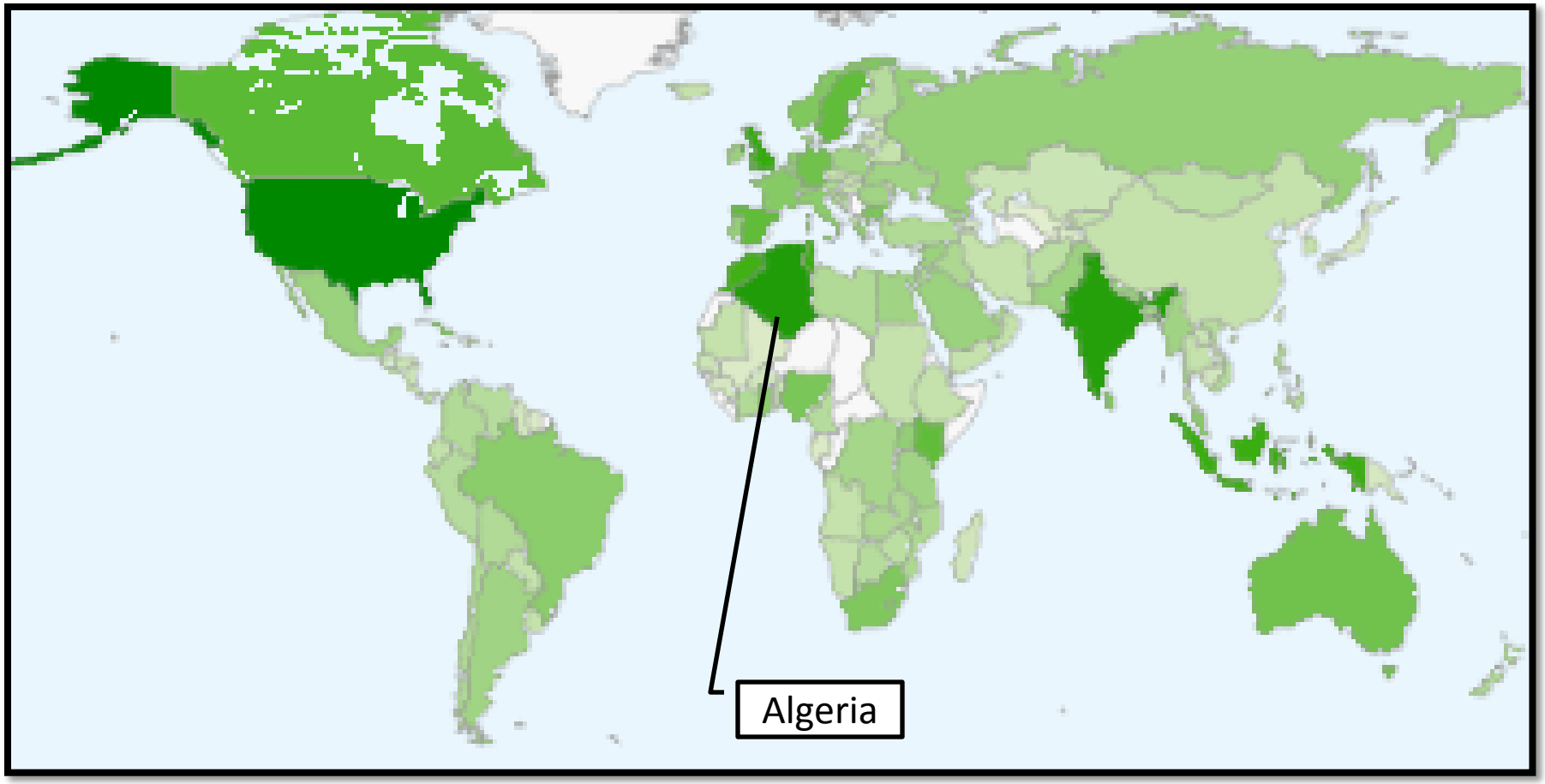
ATTACKER ID?

- Hacking Windows 7 with Metasploit



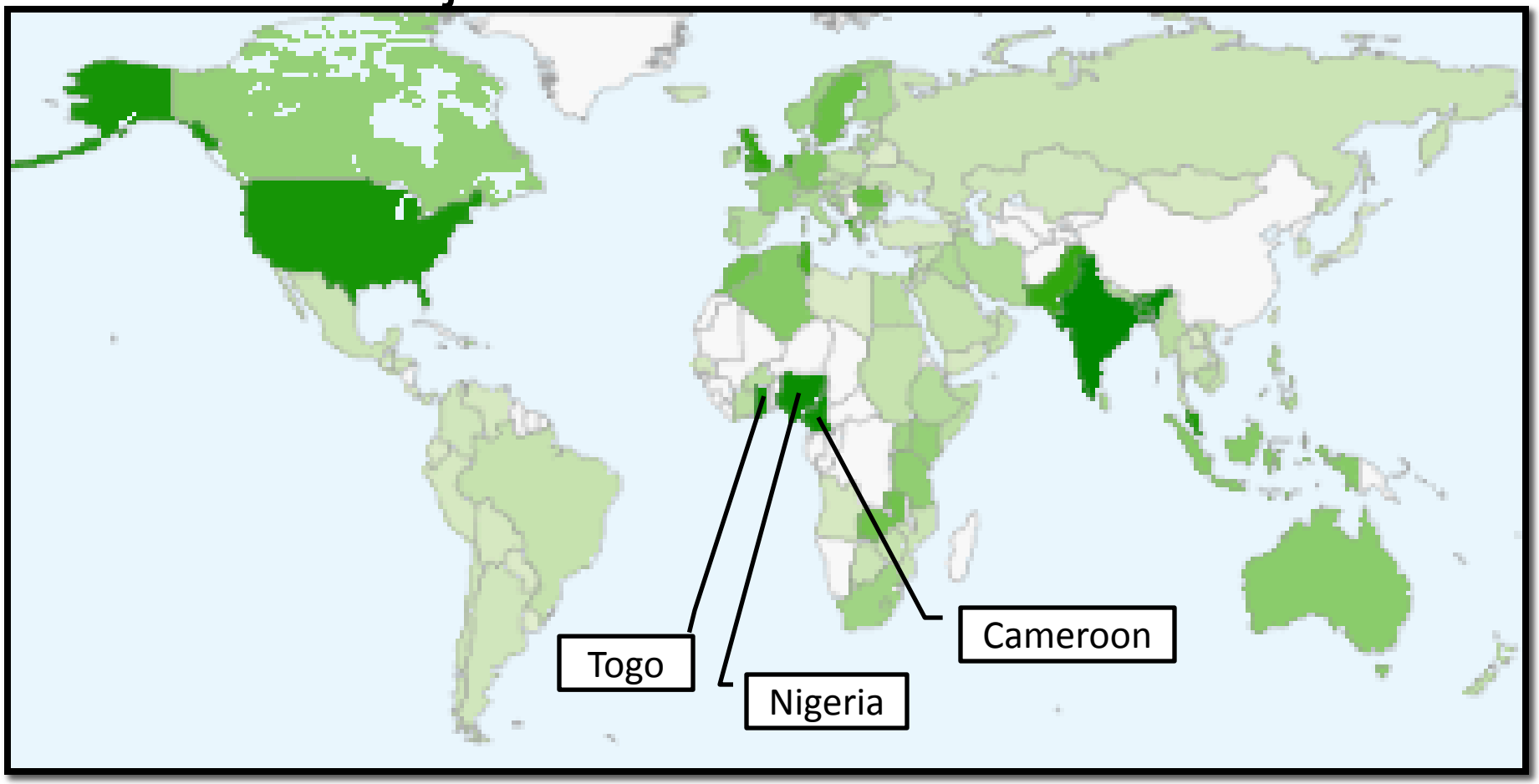
ATTACKER ID?

- Hacking using nmap nessus and metasploit



ATTACKER ID?

- Find SQL Injection Vulnerable Sites…



What it all Means

MESSAGE IN A BOTTLE

- Respond to the Four Steps
  - Consider all *material assets* when scoping
  - Spot smaller, more frequent attacks
  - Reduce incentives
- Defense Strategies
  1. Investment, Infrastructure
  2. National authority
  3. Regulation
  4. *Basic controls*

SPOT SMALLER, MORE FREQUENT ATTACKS

- Anonymous as the new auditor
  - Assessment without authorization (the Commons)
  - Super-collaboration (hacktivism) begs attribution
  - Simpler toolsets
- Insider/*End-user* highly “targeted”
  - VPN
  - Mobile (BYOD)
  - Social Networks
  - Removable Media

REDUCE INCENTIVES

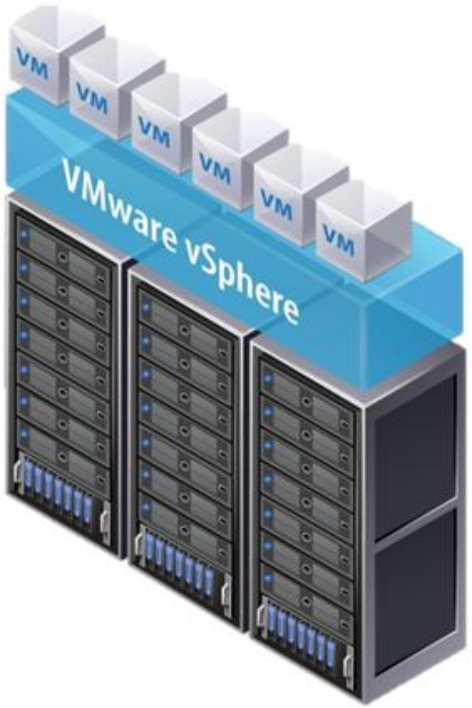
- Monitor training, kits and tools
- Look for accumulation of wealth and assets
- Track Collaboration (Increased target surface)
- Mistakes inevitable

"the [Koobface] gang's success was more attributable to workaday persistence and willingness to adapt than technical sophistication"

Increased Pressure for *Hackback*

http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf
http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-the-open.html?_r=1

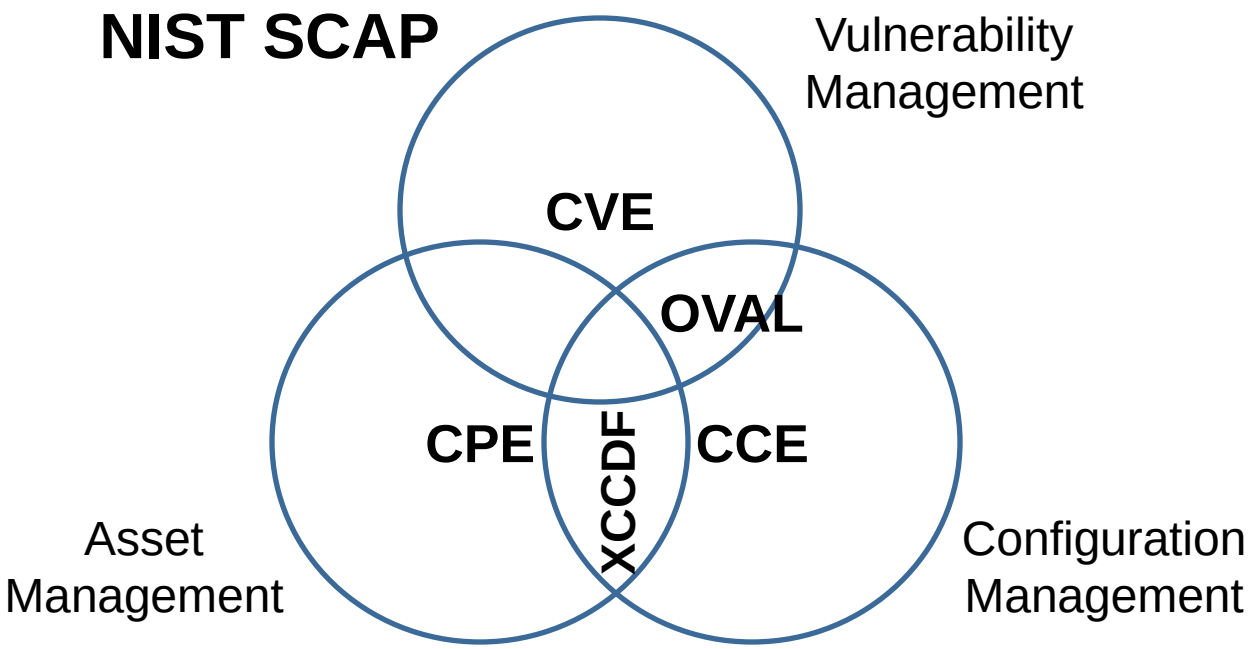
DEFENSE: VIRTUALIZATION



- Availability
  - Resilient (Decoys)
  - Flexible (Evasion)
- Integrity
  - Snapshots (Recovery Time)
  - Envelopes (OVF)
  - Non-persistence (Recovery Point)
- Confidentiality
  - Configuration/Patching Automation (SCAP)
  - Dynamic/RBAC Segmentation
  - File-level encryption

DEFENSE: AUTOMATION (C2)

1. Define standards / checklists
2. Automate management



http://scap.nist.gov/

DEFENSE: HACKBACK

1. ***Establish Legal Framework*** for Defensive Action
2. Assess Direct and Collateral Damage
3. Announce Intent and Liability for Action
4. Engage/Collaborate
5. Trackback
6. Hackback

http://www.cat-health.co.uk/advice/offensive-defense-behaviour/

Message in a Bottle: Finding Hope in a Sea of Security Breach Data

DAVI OTTENHEIMER

FLYINGPENGUIN

Session ID: DAS-302

Session Classification: Intermediate