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

**DAVI OTTENHEIMER**
**FLYINGPENGUIN**

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

# AGENDA

- Background
- Data Analysis
- Message

# Background

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

flyingpenguin
the poetry of information security

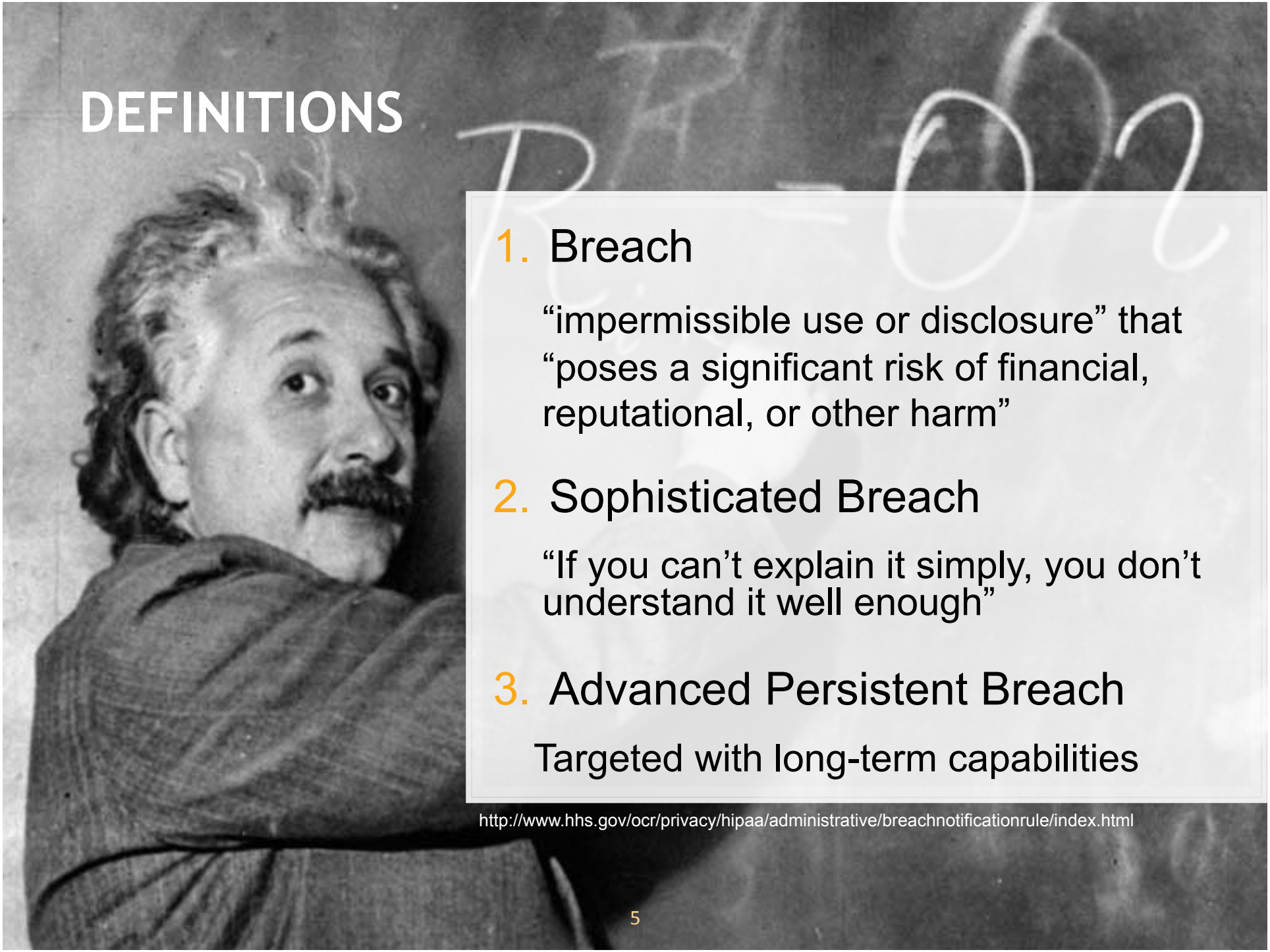
flying \fly"ing\, a. [From fly, v. i.]

*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*

# 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

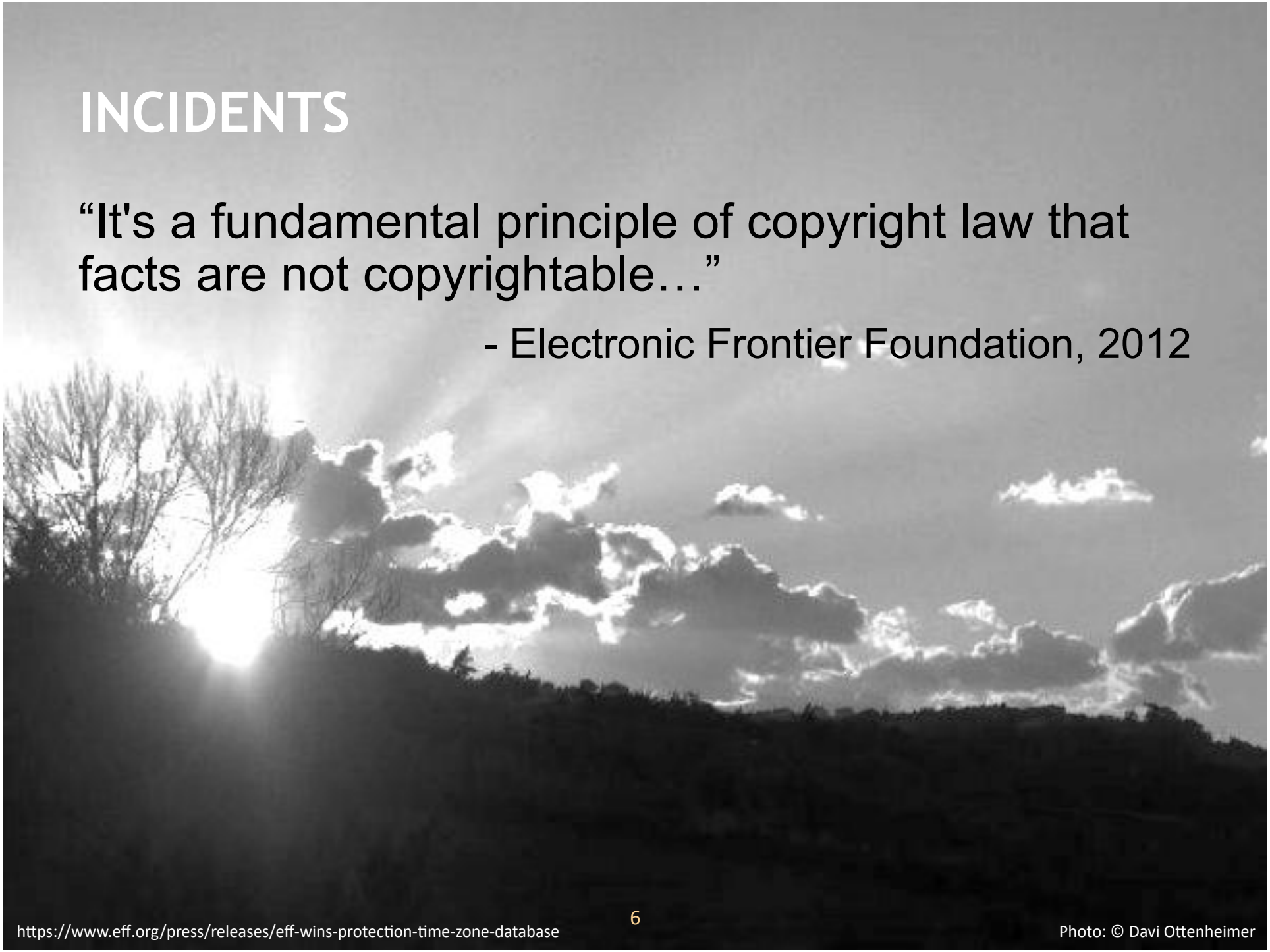
   Targeted with long-term capabilities

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

# INCIDENTS

"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

# INVESTIGATORS/REPORTS

- 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

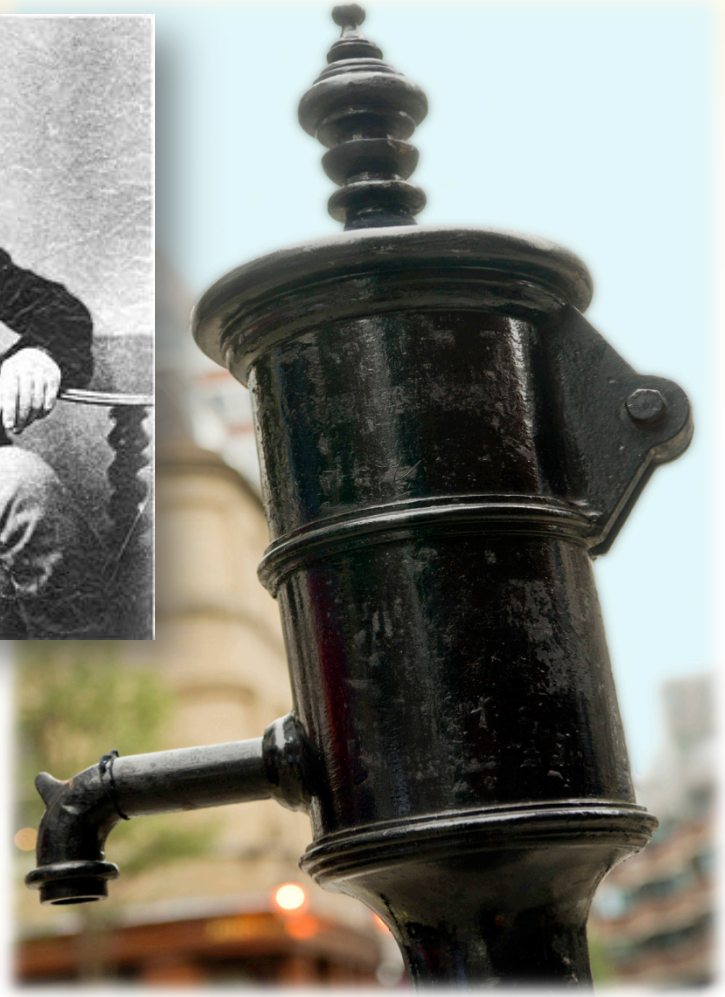
- 40 Breaches reported in Q4
- Spam and malware in *decline*
- Mobile malware rising
- Malicious URLs up 8x in 2011
- 73% of malicious content hosted in the US

# Data Analysis

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

# EPIDEMIOLOGY

- 1854 Cholera Epidemic
- Dr. Snow's "Ghost map"
- Authorities convinced to remove pump handle



http://secretldn.wordpress.com/2011/09/10/the-broad-street-pump/

# GHOST MAP

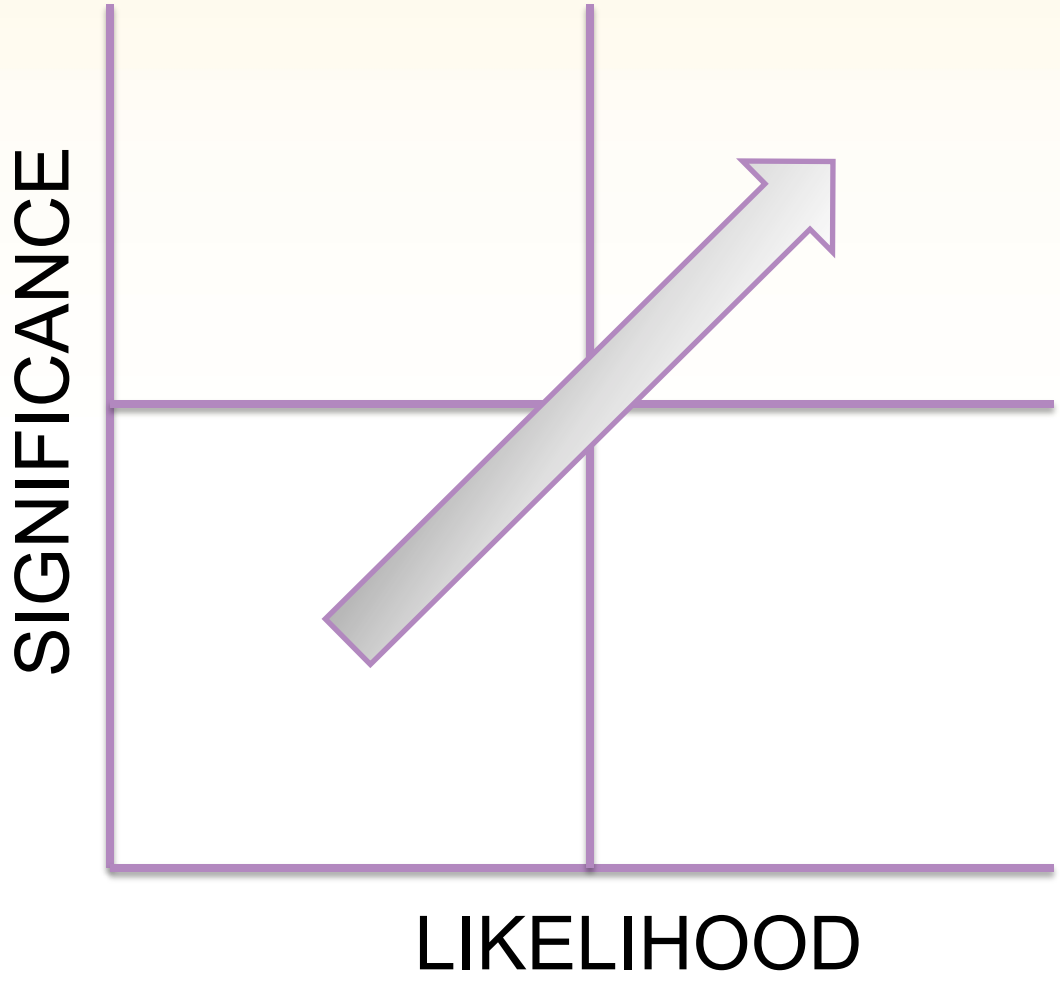
• = Deaths

✖ = Pump



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

# ANALYSIS OF DATA



# SIGNIFICANCE

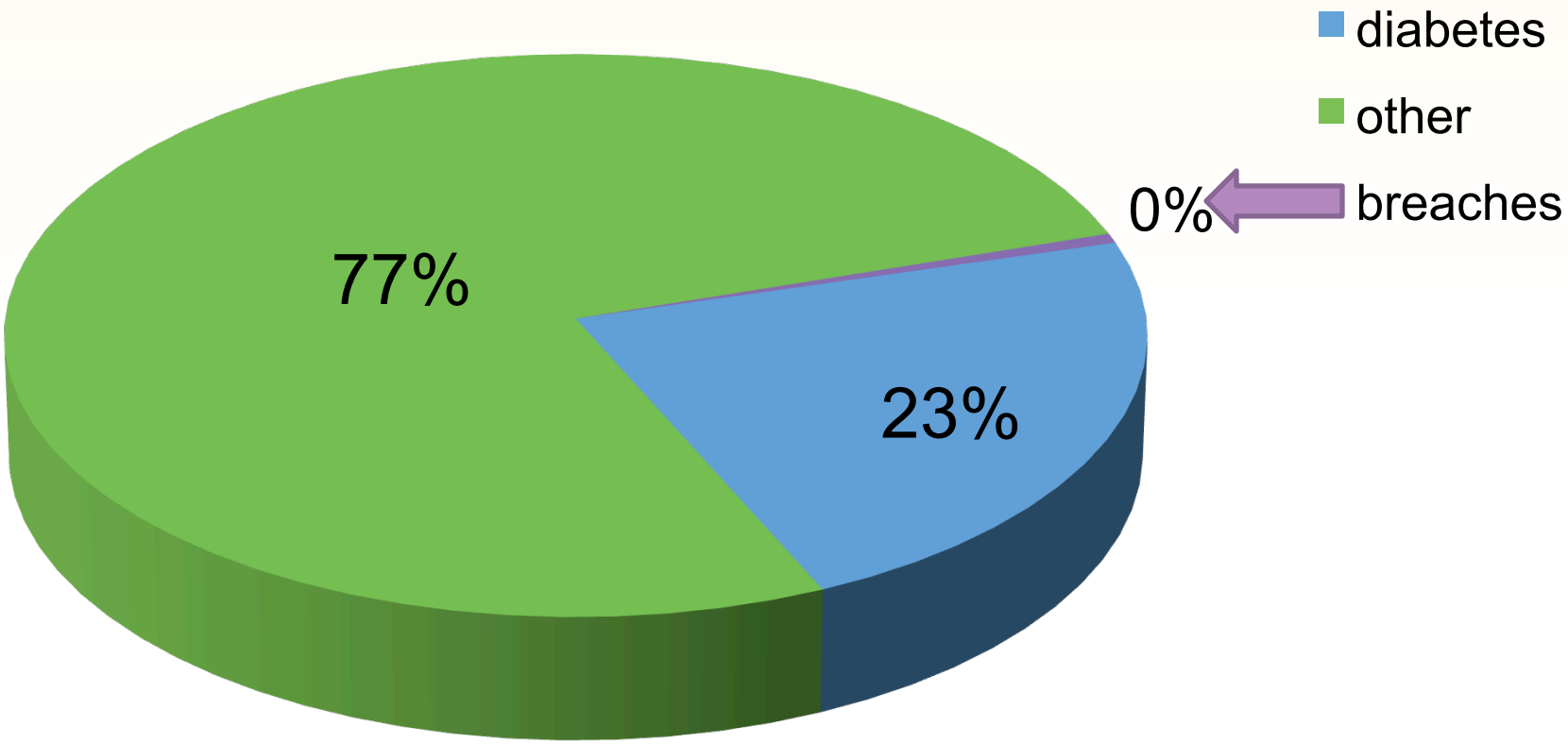
| Billions | vs. | 83 Billion |
|---|---|---|
| "New study shows **data breaches** up and costing healthcare industry **billions of dollars a year**, with employees, mobile devices the weakest link." | | "…according to a report released last week from the Agency for Healthcare Research and Quality (AHRQ), **[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

# SIGNIFICANCE

**Billions vs. 83 Billion**
Healthcare Costs to Americans



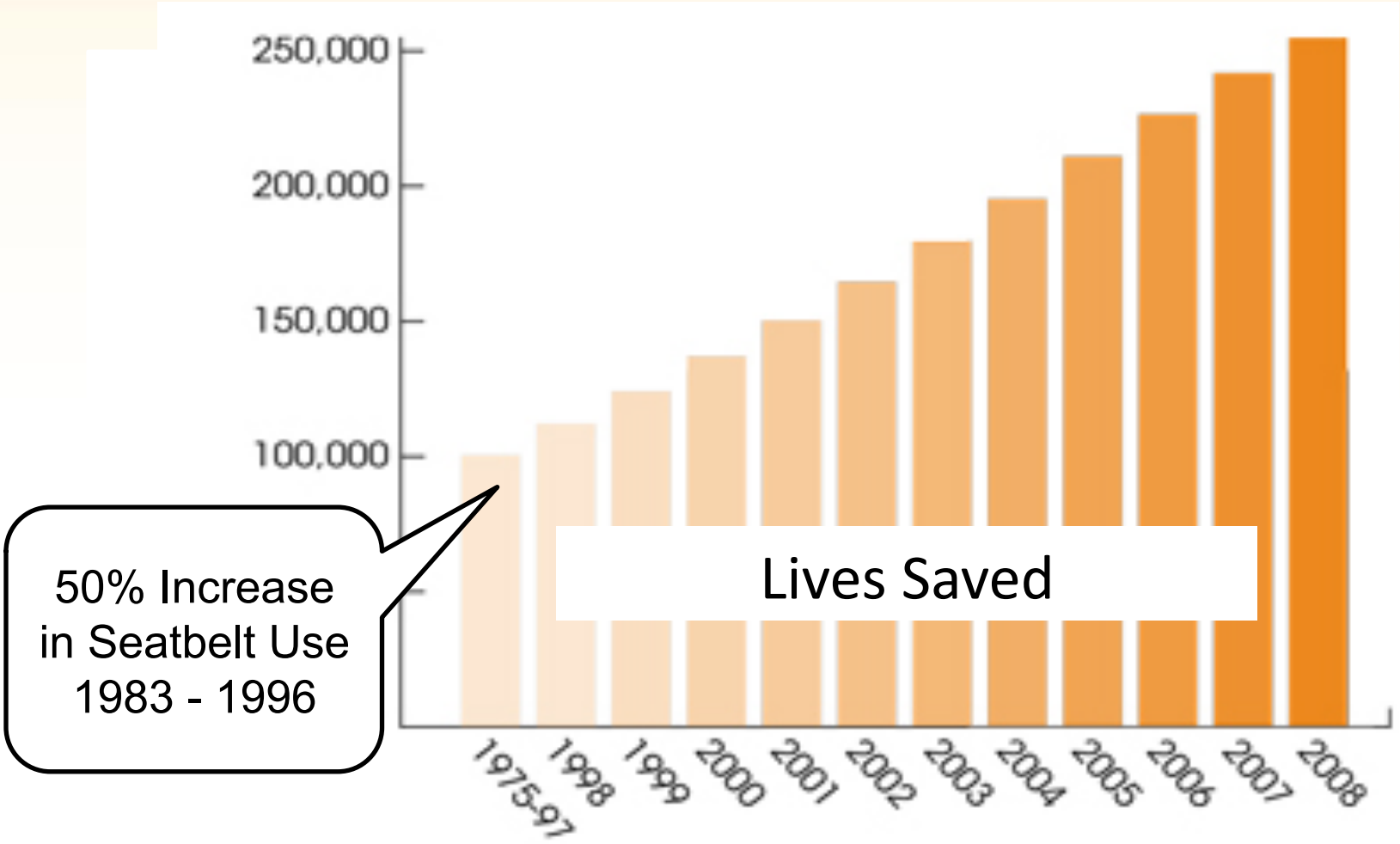
# LIKELIHOOD OF RISK (LOSS)


## CAR RACING

- 1911 Aerodynamics
- 1911 Rear-view mirror
- 1921 4 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/

# LIKELIHOOD




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

# LIKELIHOOD

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

- Improved strength for $500 = 3%
- Better road signage = 8%
- Airbag = 10-25%

  (297 lbs of structure, 12 yr younger)

50%

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

# Message

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

# 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

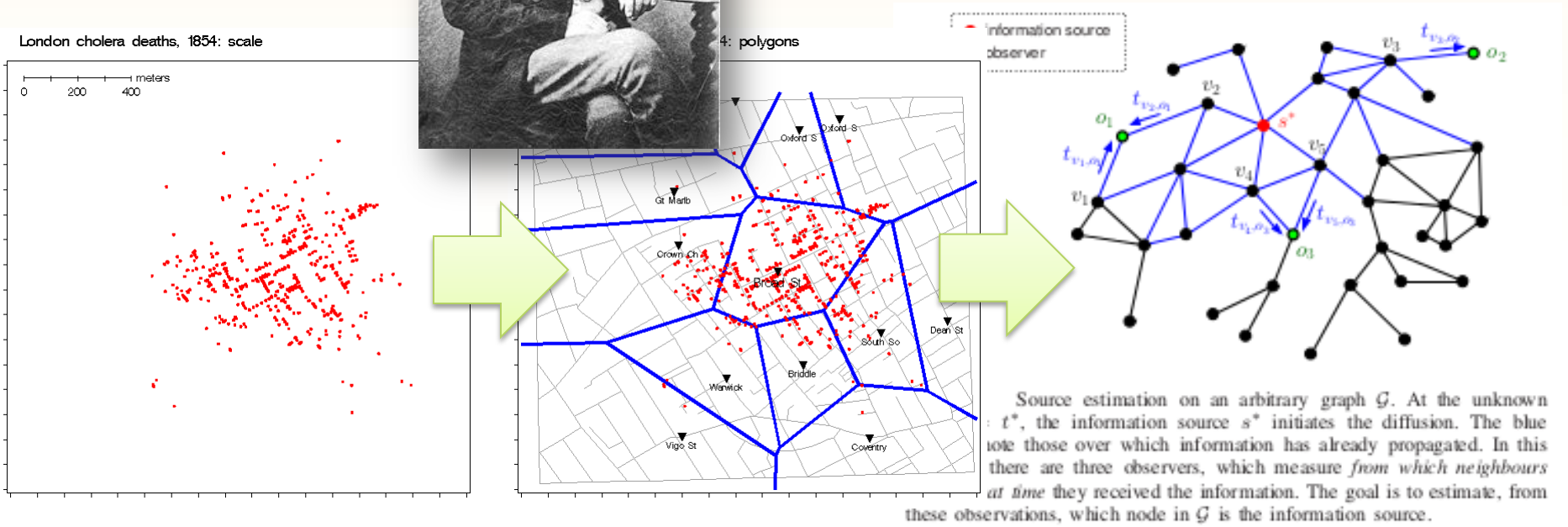
- External – 92% of Breaches, 99% of Records
- Internal – 17% of Breaches, 1% of Records
  - 85% end-user
  - 22% finance/accounting
- Partners – 0% (down from 22% in 2010)
- Causes
  - Malware 49%
  - Hacking 50%
  - Physical 29%

(Social Network Attacks only 5% of Social Engineering)

# VERIZON

- Patch In 5-6 mos, AV 8-9 days = < 10% benefit
- 85% Externally notified
- Risk 60% lower if ***response sub 2 hours***
- No new cat. of attack – ***scan for just 5 ports***
- 4.7 steps per attack – ***only need to stop one***

# MESSAGE




Source estimation on an arbitrary graph $\mathcal{G}$. At the unknown $t^*$, the information source $s^*$ initiates the diffusion. The blue note those over which information has already propagated. In this there are three observers, which measure *from which neighbours at time* they received the information. The goal is to estimate, from these observations, which node in $\mathcal{G}$ is the information source.

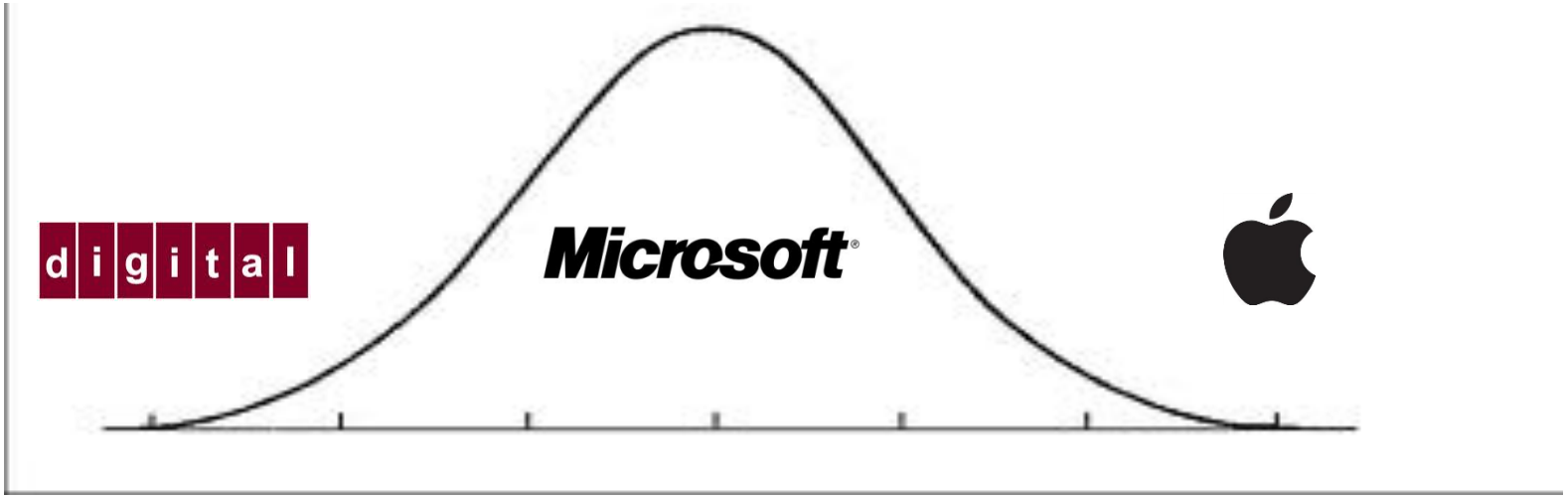
http://www.datavis.ca/gallery/historical.php
http://www.pedropinto.org.s3.amazonaws.com/publications/locating_source_diffusion_networks.pdf

# MESSAGE

1. Perimeters work, but limited (e.g. seatbelts)
2. Attackers focus 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***

# MESSAGE

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



# MESSAGE

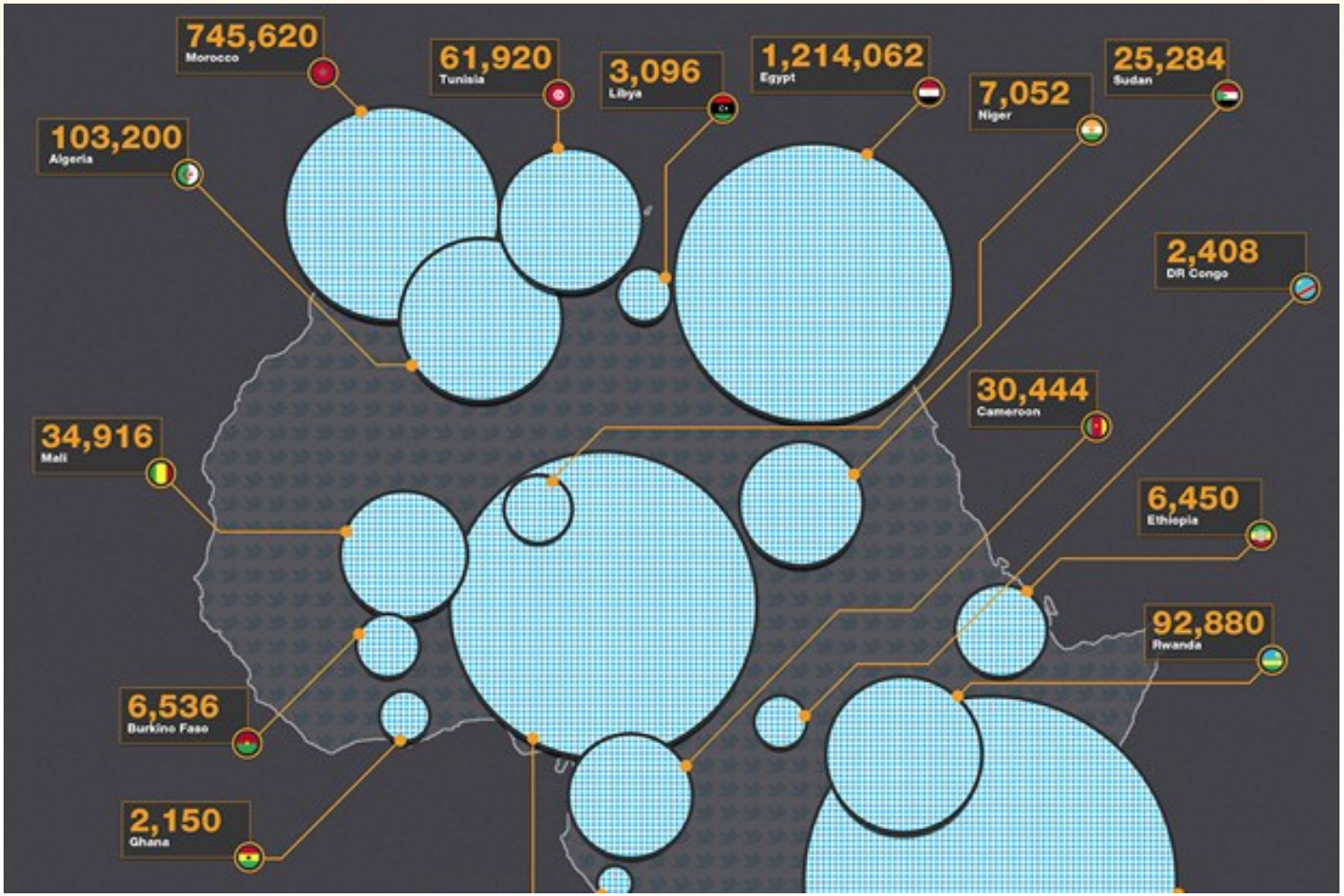
## WHERE TO SPEND

1. Manage Identities
   - Default/Guess
   - Weak
2. Prevent and Detect SQL Injection
3. Manage Configurations
4. Expand Scope to Non-critical Systems

# WHAT IF

- Attackers make the same mistakes…
- We reverse the methodology
- We expand our scope
- We correlate data

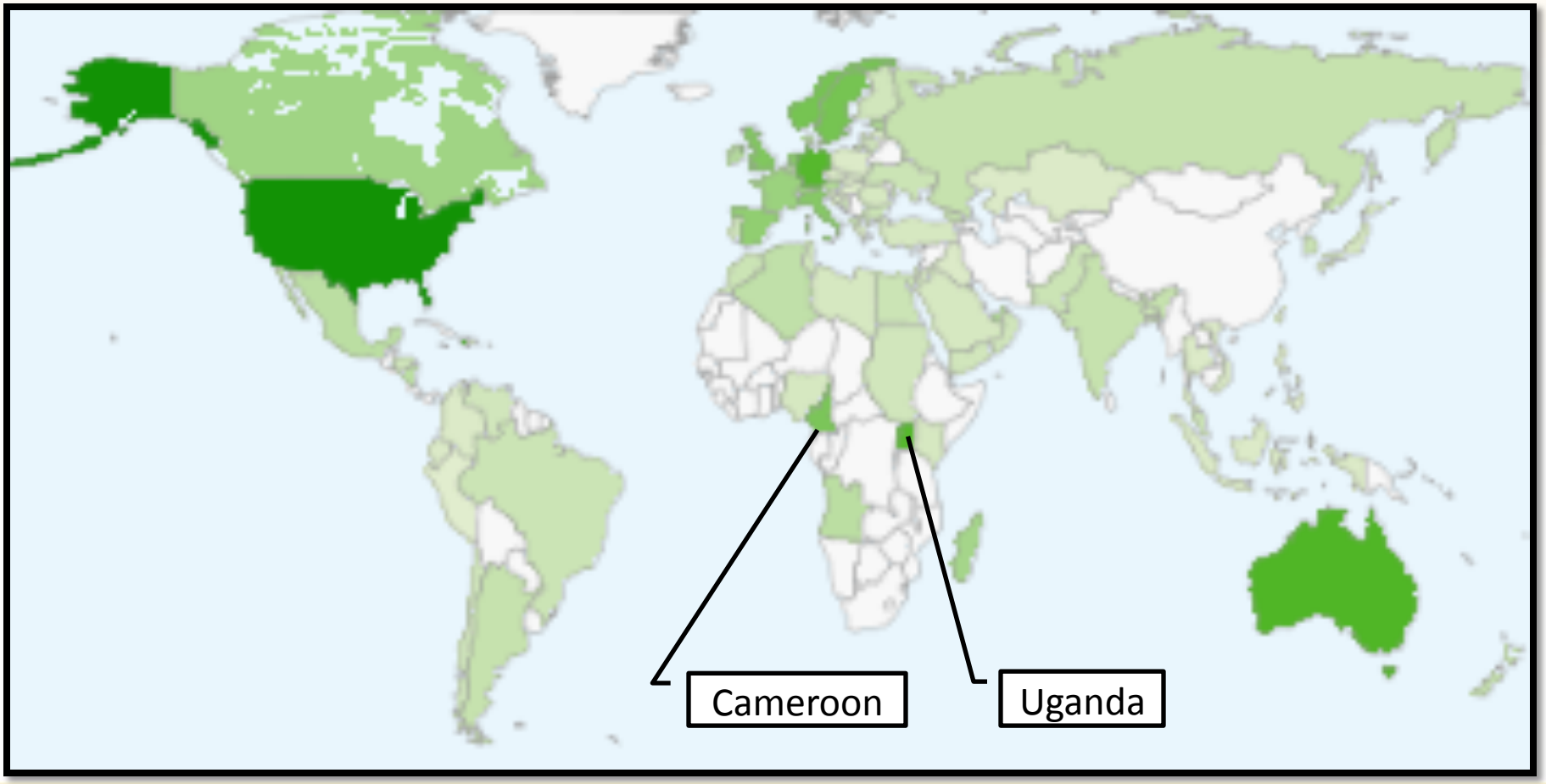
# 12 MILLION TWEETS, OCT-DEC '11




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

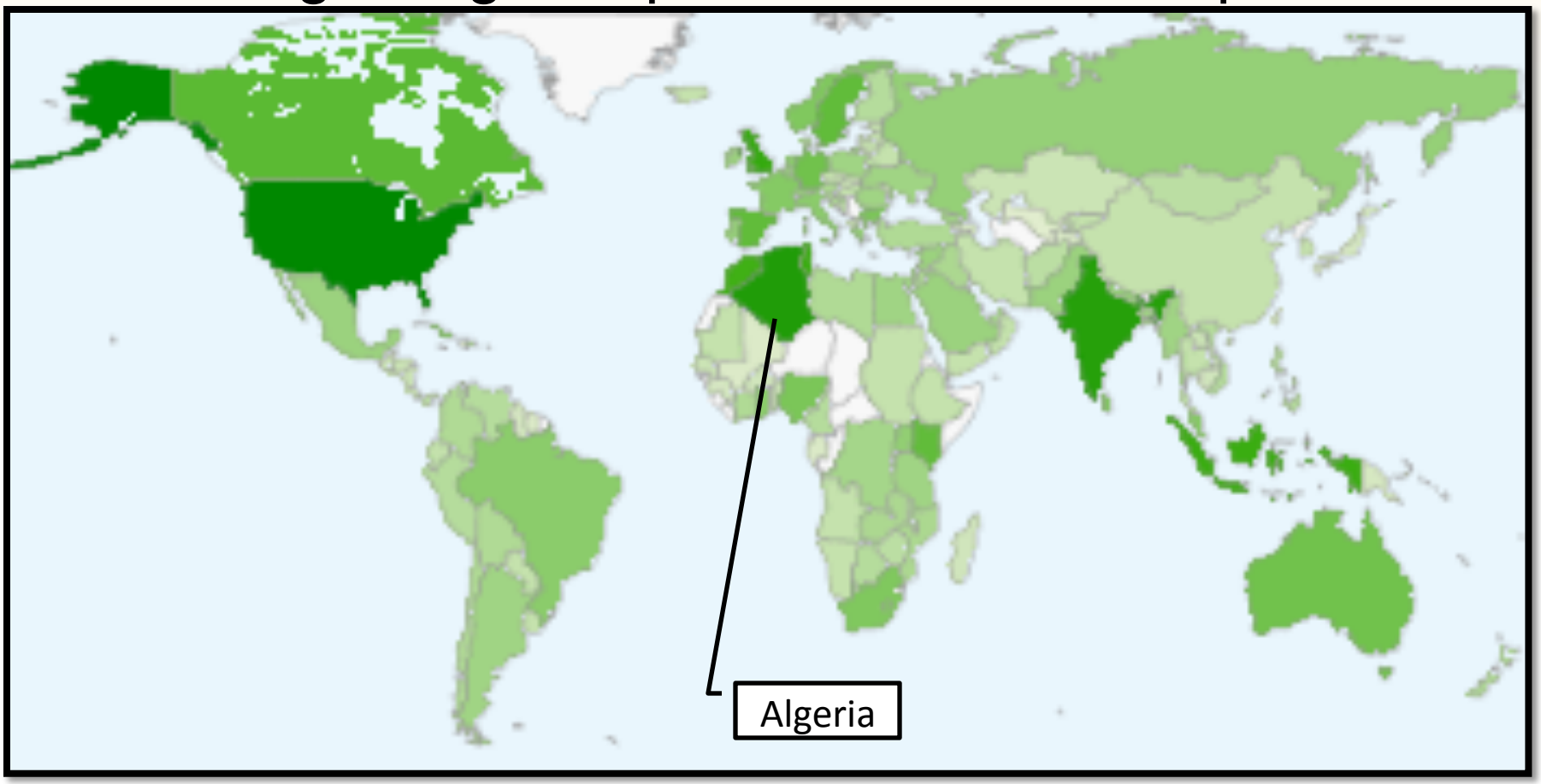
# WHO IS TRAINING ON WHAT?

- Black Hole RAT Tutorial



# WHO IS TRAINING ON WHAT?

- Hacking using nmap nessus and metasploit



# ACTIVE DEFENSE

- Monitor (Training, Kits and Tools)
- Alert on Anomaly (Wealth and Assets)
- Engage Based on Data

  “the [Koobface] gang’s success was more attributable to workaday persistence and willingness to adapt than technical sophistication”

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

# ACTIVE DEFENSE

1. **Establish Legal Framework**
2. Calculate Direct and Collateral Damage
3. Declare Intent and Liability
4. Collaborate and Collect Data
5. **Actively Defend**

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

**DAVI OTTENHEIMER**
**FLYINGPENGUIN**

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012