瓶中信：
在安全违规数据的
汪洋大海中寻找希望

DAVI OTTENHEIMER
FLYINGPENGUIN

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

会话 ID：
会话分类：

议程

- 背景
- 数据分析
- 启示

背景

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

flyingpenguin
the poetry of information security

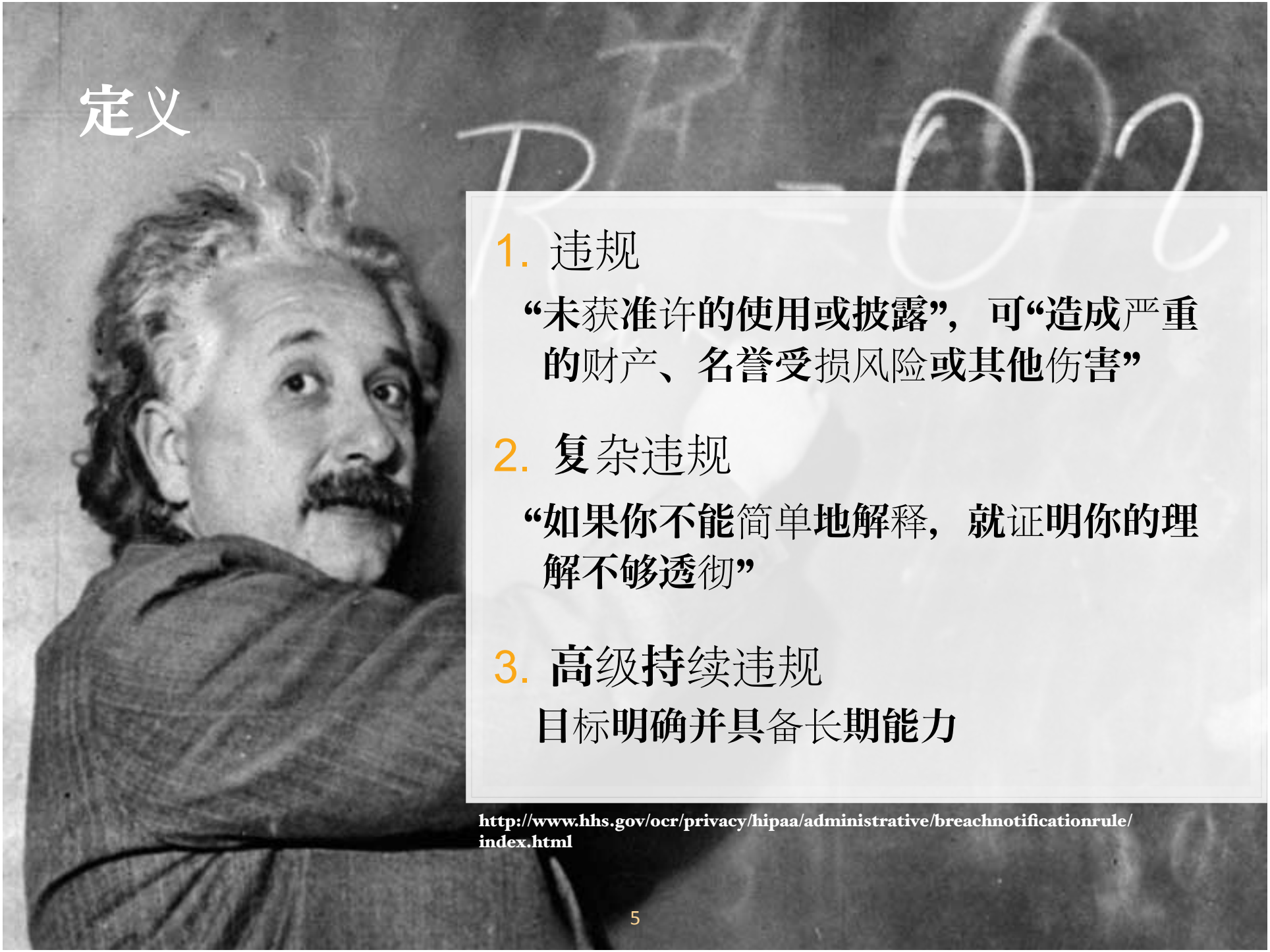
flying（飞行）\fly"ing\, a. [源于 fly， v.i.]

用翅膀或像用翅膀一样移动；轻快或快速地移动；用于表示快速移动

penguin（企鹅）\pen"guin\, n.

生活在南半球寒带地区特别是南极洲的一种短腿不能飞翔的鸟类动物，长有适合在水中生活的蹼足和鳍状翼

定义



1. 违规

   “未获准许的使用或披露”，可“造成严重的财产、名誉受损风险或其他伤害”

2. 复杂违规

   “如果你不能简单地解释，就证明你的理解不够透彻”

3. 高级持续违规

   目标明确并具备长期能力

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

事件

“事实是不受版权保护的，这是版权法的一项基本原则…”

- Electronic Frontier Foundation，2012 年

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

照片：版权所有 Davi Ottenheimer

调查公司/报告

- **Trustwave**
- **Verizon**
- **Trend Micro**
- **Sophos**
- **McAfee**
- **Dell SecureWorks**
- **AlienVault**
- **Secunia**

- Ponemon
- US States (NCSL)
- privacyrights.org
- 身份盗窃资源中心
- **HHS.gov**

“根据 HITECH 法案 13402(e)(4) 一节中的要求，部长必须发布清单，列出影响人数超过 500 人的受保护健康信息因安全保护不力而导致的泄露事件。”

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

2012 年 WP 全球安全保护报告

- 300 项调查
- 18 个国家/地区
- 20% 的不明侵入方法
- 33% 的不明源头

VERIZON

2011 年数据泄露调查报告

- 834 个案例（40% 为医院，25% 为零售业，22% 为金融服务）
- 33,000 个攻击步骤
- 54 例代理/行动交叉
- 威胁源头
  - 3%：中国（若算上最后一跳则为 50%）
  - 65%：东欧
  - 19%：北美
  - 12%：未知

TREND MICRO

2011 年回顾：信息就是金钱

- “数据泄露年”
  - 漏洞更少，攻击更复杂
    - 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
  - “无知的用户总会犯错误，不管他们进入什么样的社交网络”
- 每秒钟都有 3.5 个新威胁被创造出来
- 垃圾邮件泛滥最严重的国家：印度 18%，俄罗斯 15%

“Lurid” Downloader（2002 年以后称 Enfal）

SOPHOS

2012 年安全威胁报告

- 80% 被感染的网站是合法网站
- 67% 的侦测涉及重定向
- 移动设备、社交网络、可移动介质

"像修补 [Conficker] 和密码管理这样的基本安全保护将是一项巨大难题"

- 垃圾邮件泛滥最严重的国家：美国 12%，印度 8%
- 垃圾邮件泛滥最严重的洲：亚洲 45%，欧洲 26%
- 受攻击 PC 数量最多的国家：智利、中国、韩国

MCAFEE

McAfee 威胁报告：2011 年第 4 季度

- 第 4 季度报告了 40 起泄漏事件
- 垃圾邮件和恶意软件数量下降
- 移动设备恶意软件数量上升
- 恶意 URL 在 2011 年增加了 8 倍
- 73% 的恶意内容寄居在美国

数据分析

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

流行病学

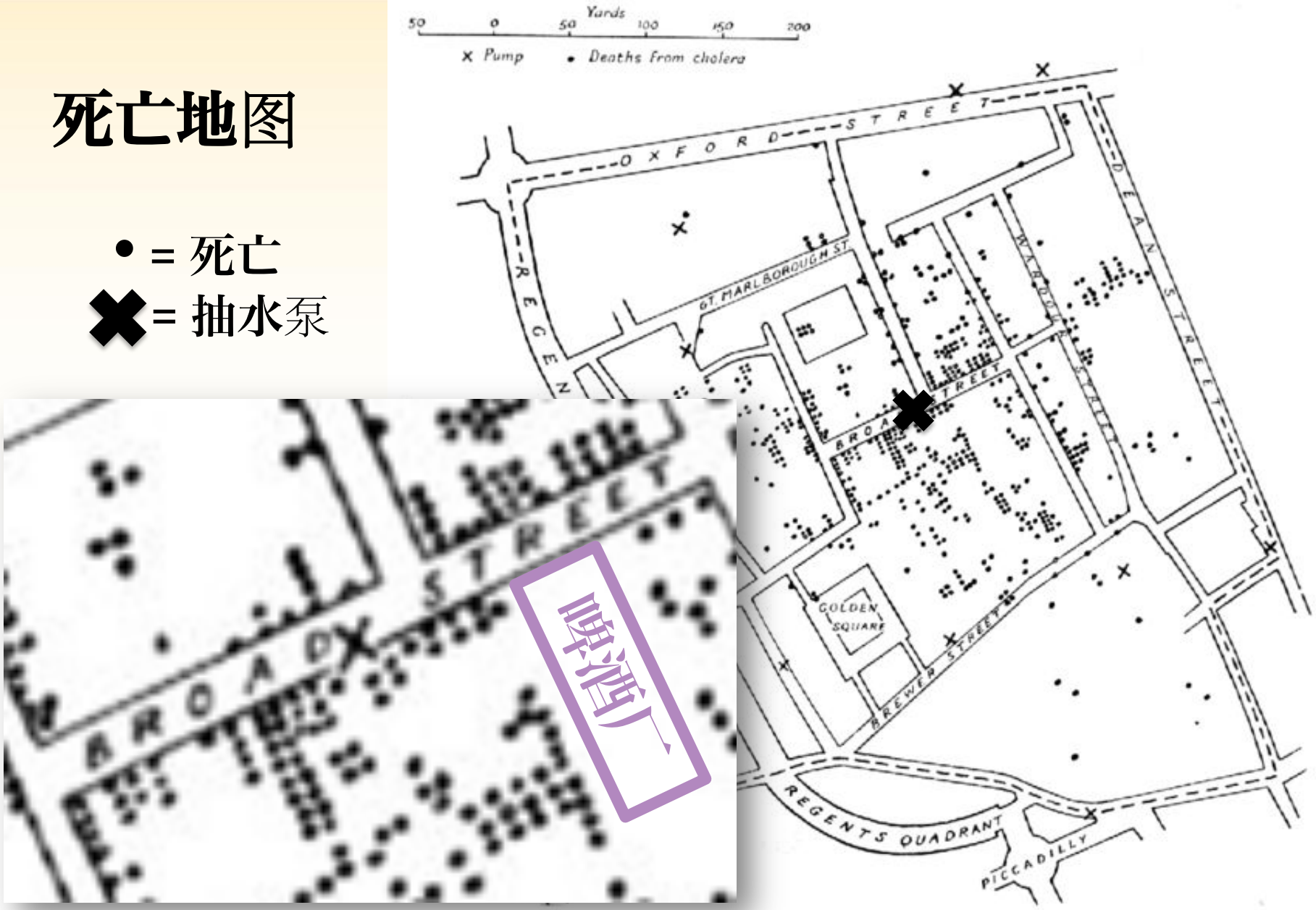
- 1854 年霍乱流行
- 斯诺医生的“Ghost map”（死亡地图）
- 说服当局卸下抽水泵的手柄

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

死亡地图

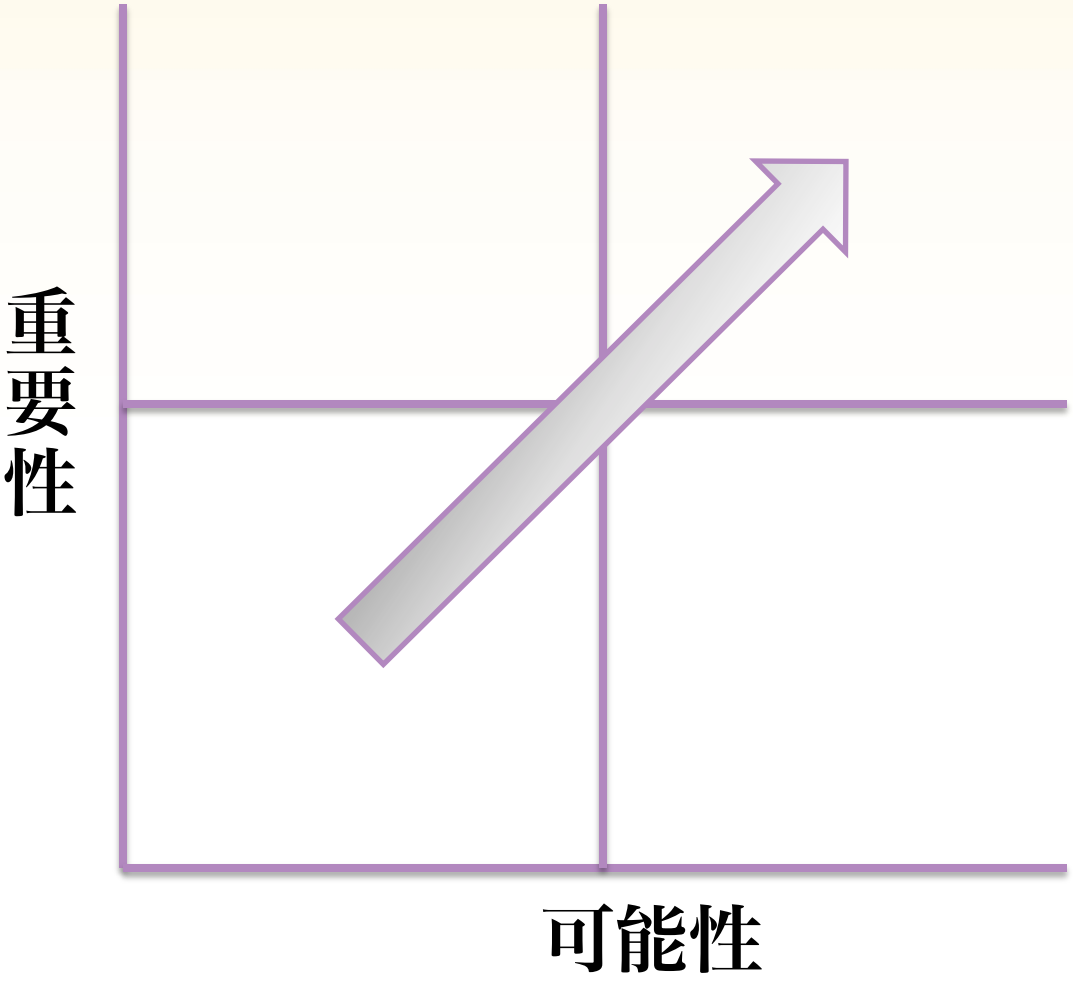
● = 死亡

✖ = 抽水泵



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

数据分析



重要性

数十亿 与 830 亿

“新的研究表明数据泄漏一年会给医疗保健行业造成数十亿美元的损失，其中员工和移动设备是最薄弱的环节。”

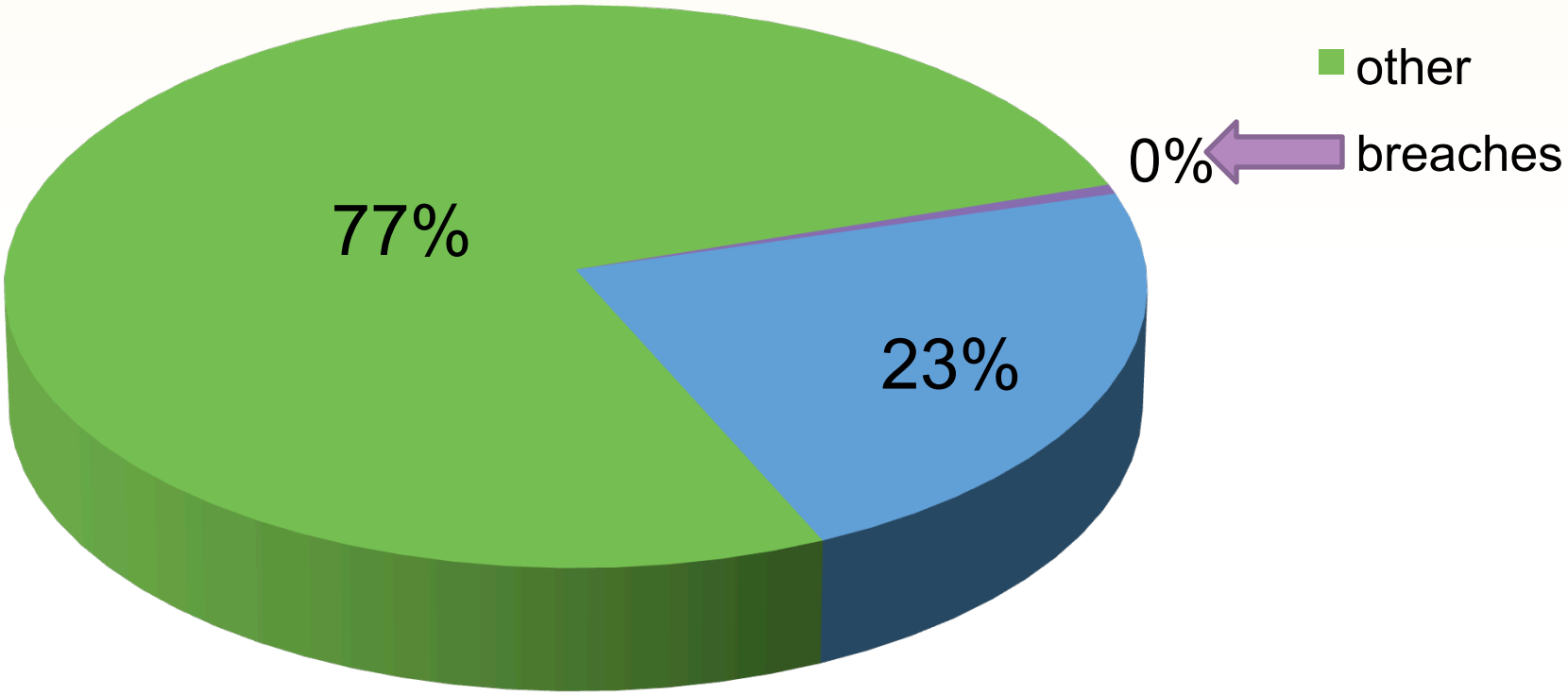
“...根据美国卫生保健研究与质量管理处 (AHRQ) 上周发布的一份报告，[糖尿病] 让美国人一年花去 830 亿美元的医疗费 — 占总医疗开支的 23%。”

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

重要性

数十亿 与 830 亿
美国人的医疗成本



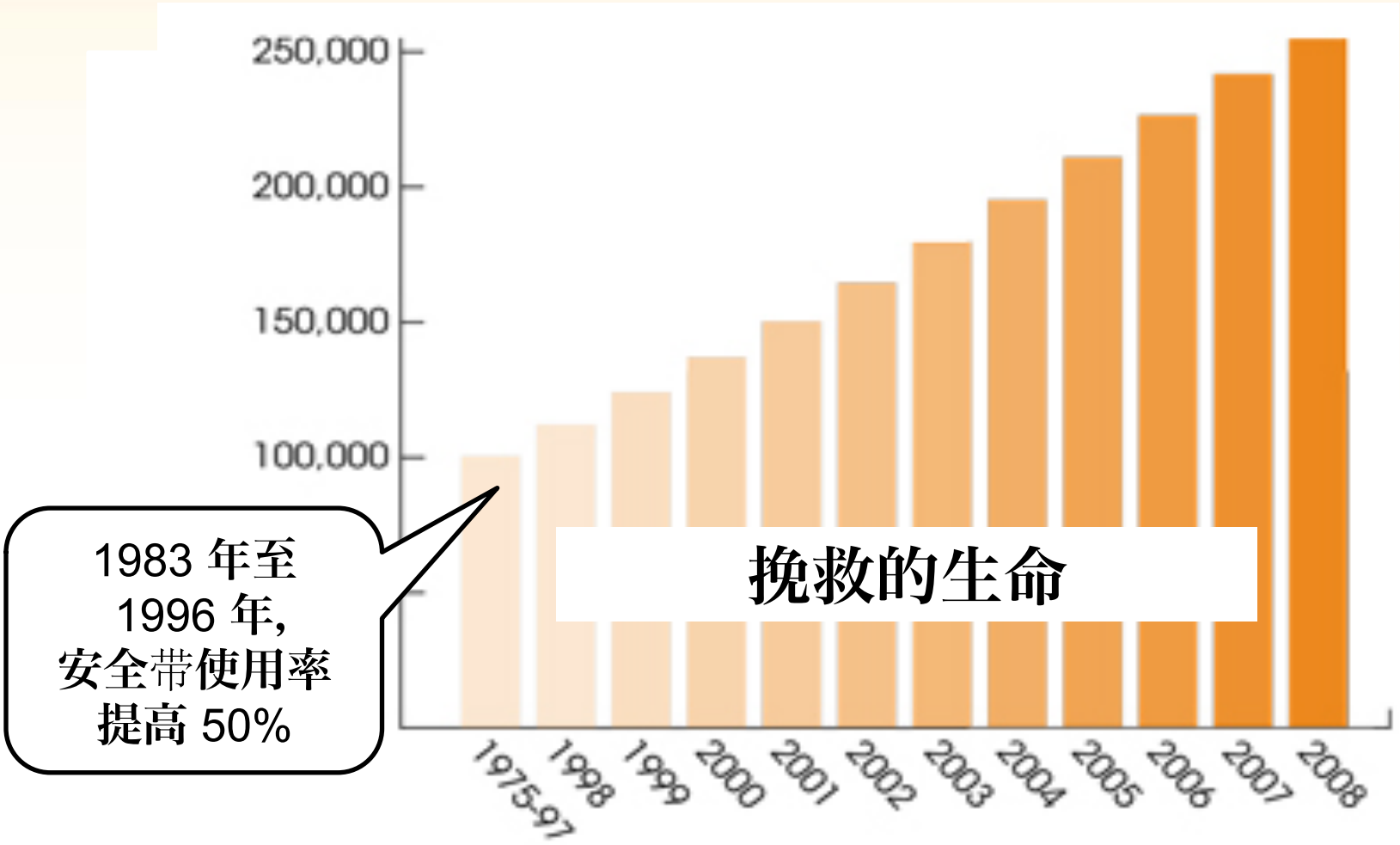
风险（损失）可能性

汽车赛

- 1911 年：空气动力学
- 1911 年：后视镜
- 1921 年：4 个液压刹车
- 1924 年：前轮驱动
- 1932 年：四轮驱动
- 1952 年：涡轮增压器
- **1956：安全带**

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/

可能性



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

可能性

“安全带将撞车时造成死亡或重伤的风险降低 50%”

- 花 500 美元增加强度 = 3%
- 改善路牌指示 = 8%
- 安全气囊 = 10-25%

  （增加 297 磅的结构，年轻 12 岁）

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

启示

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

TRUSTWAVE SPIDERLABS

- 78% 在食品和饮料业 + 零售业
- 89% 为客户记录
- 76% 与合作伙伴有关
- 外部侦测（执法部门）的数量增加 5 倍
- 88% 的恶意软件未被检测到（12% 的有效率）
- SQL 注入是第一号攻击
- Password1 b/c “满足默认 AD 要求”

VERIZON

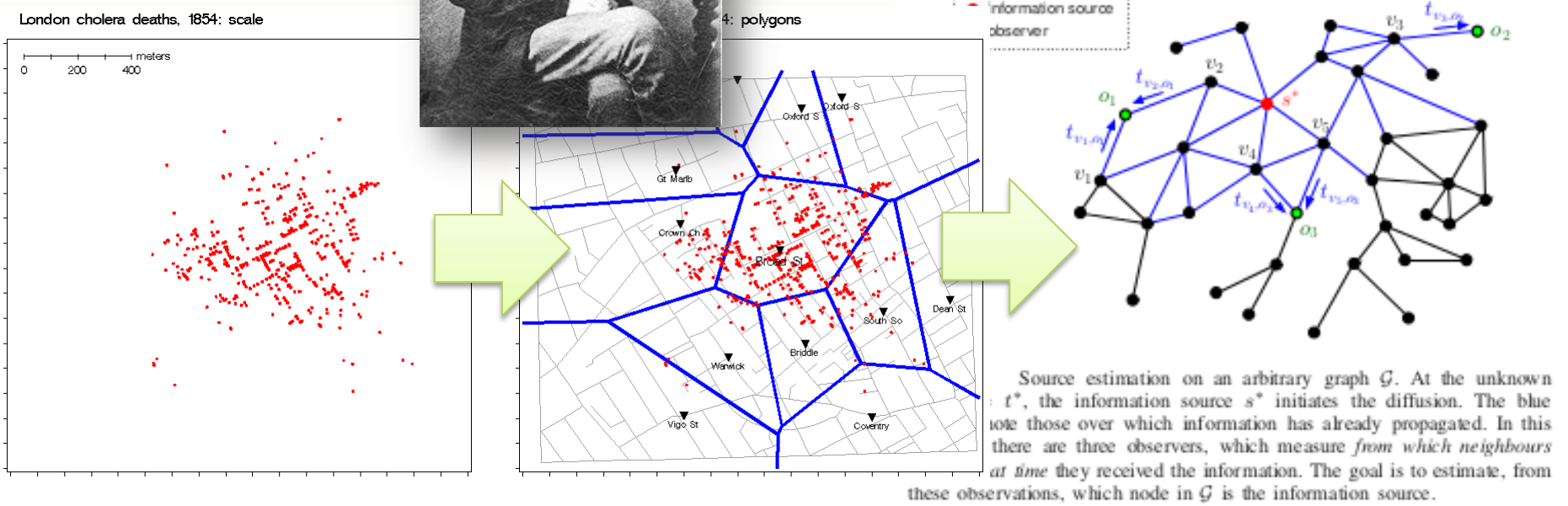
- 外部 – 92% 的违规，99% 的记录
- 内部 – 17% 的违规，1% 的记录
  - 85% 为终端用户
  - 22% 为财务/会计部门
- 合作伙伴 – 0%（2010 年为 22%）
- 原因
  - 恶意软件 49%
  - 黑客 50%
  - 物理 29%

（社交网络攻击仅占社会工程学攻击的 5%）

VERIZON

- 每 5-6 个月修补一次，每 8-9 天进行一次用户身份验证 = 获得的好处不到 10%
- 85% 由外部获得通知
- 风险降低 60% – *如果在 2 小时内响应*
- 无新的攻击类别 – *只需扫描 5 个端口*
- 每一例攻击平均 4.7 个步骤 – *只需阻止其中一个步骤*

启示



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

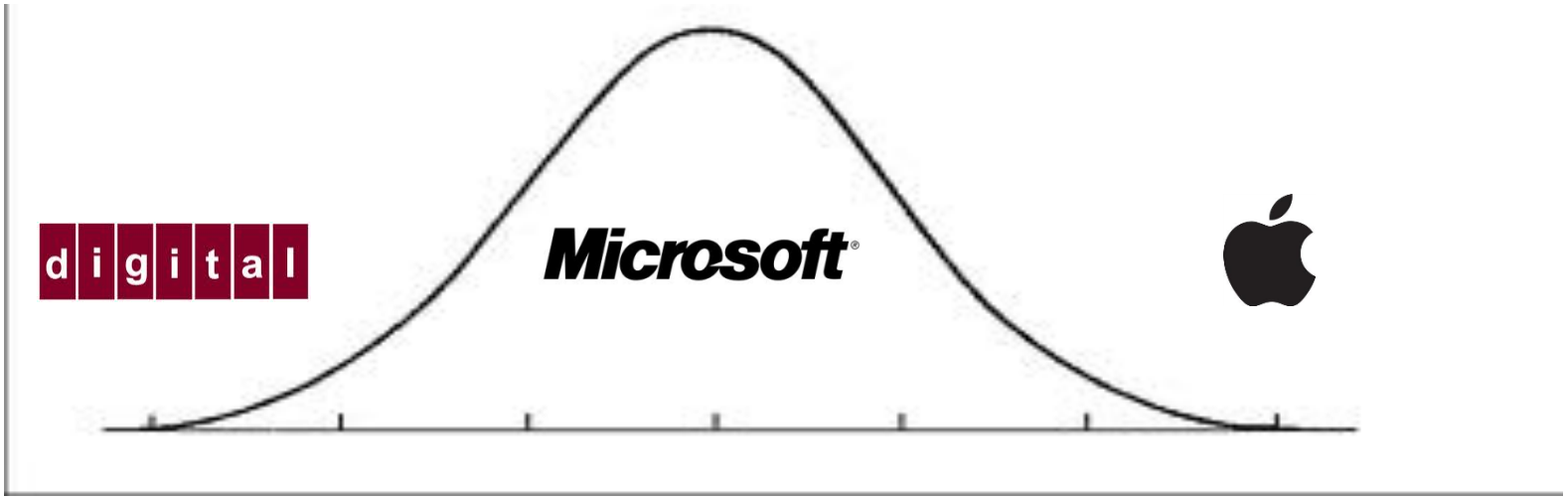
http://www.datavis.ca/gallery/historical.php
http://www.pedropinto.org.s3.amazonaws.com/publications/locating_source_diffusion_networks.pdf

启示

1. 外围防御有效，但效果有限（例如安全带）
2. 攻击者主要是寻找*例外*
   - VPN（令牌）
   - 苹果和安卓 (BYOD)
   - 不常见的服务（后门）
   - 出站端口（80、443、25）
   - 终端用户界面（社会决策/覆盖）
3. 每一项资产都是目标
4. 攻击源头多为未知，但具有*社会性*

启示

1. 默认或较弱的凭据
2. 缺少输入过滤（包括，注入）
3. 过多服务
4. 未修补的系统（旧式系统和新购系统）



启示

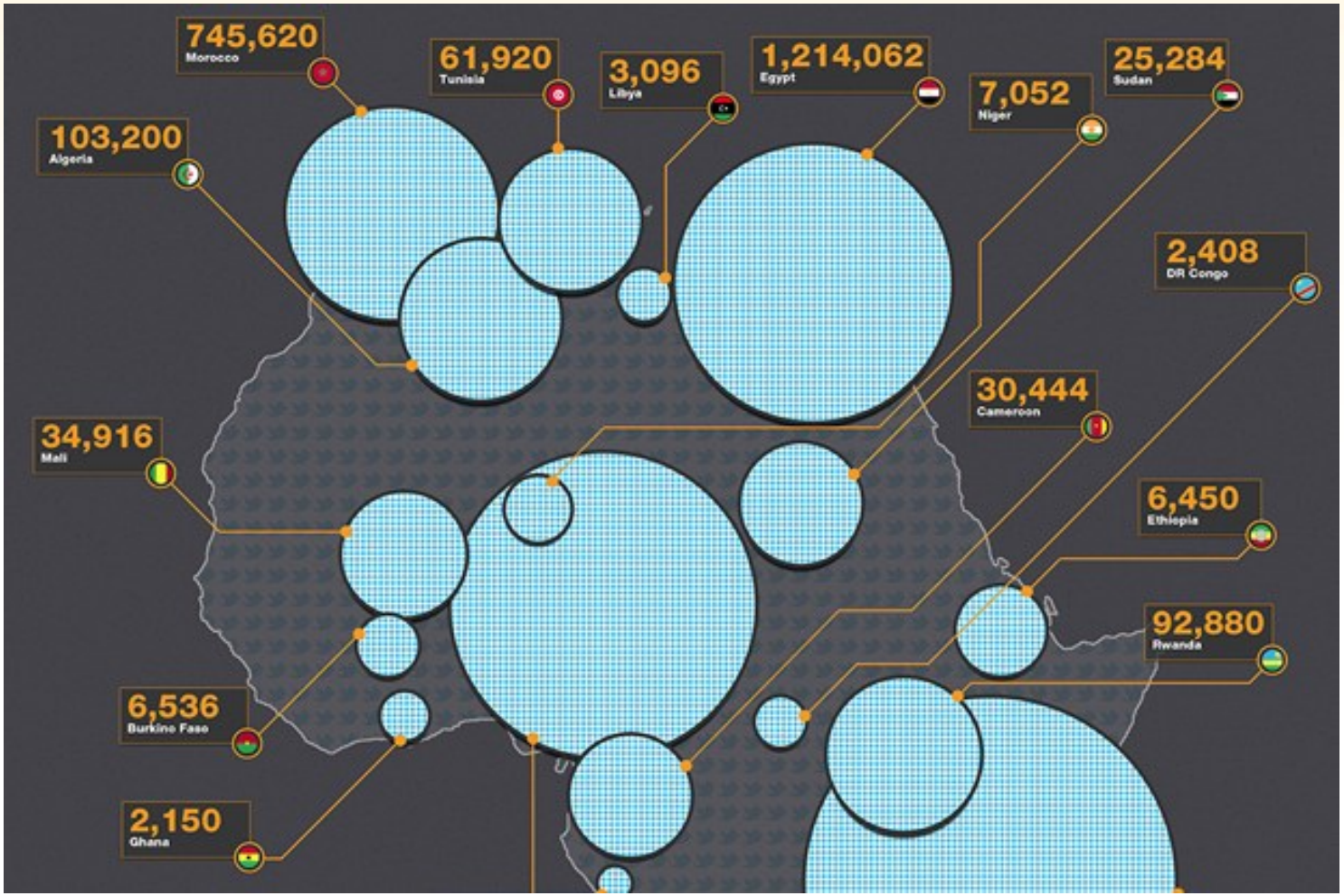
精力应放在哪里

1. 管理身份
   - 默认/猜测
   - 弱
2. 预防和检测 SQL 注入
3. 管理配置
4. 将范围扩大到非关键系统

假如

- 攻击者犯同样的错误…
- 我们逆向执行我们的方法
- 我们扩大范围
- 我们关联数据

1200 万 Twitter 信息，2011 年 10 月至 12 月

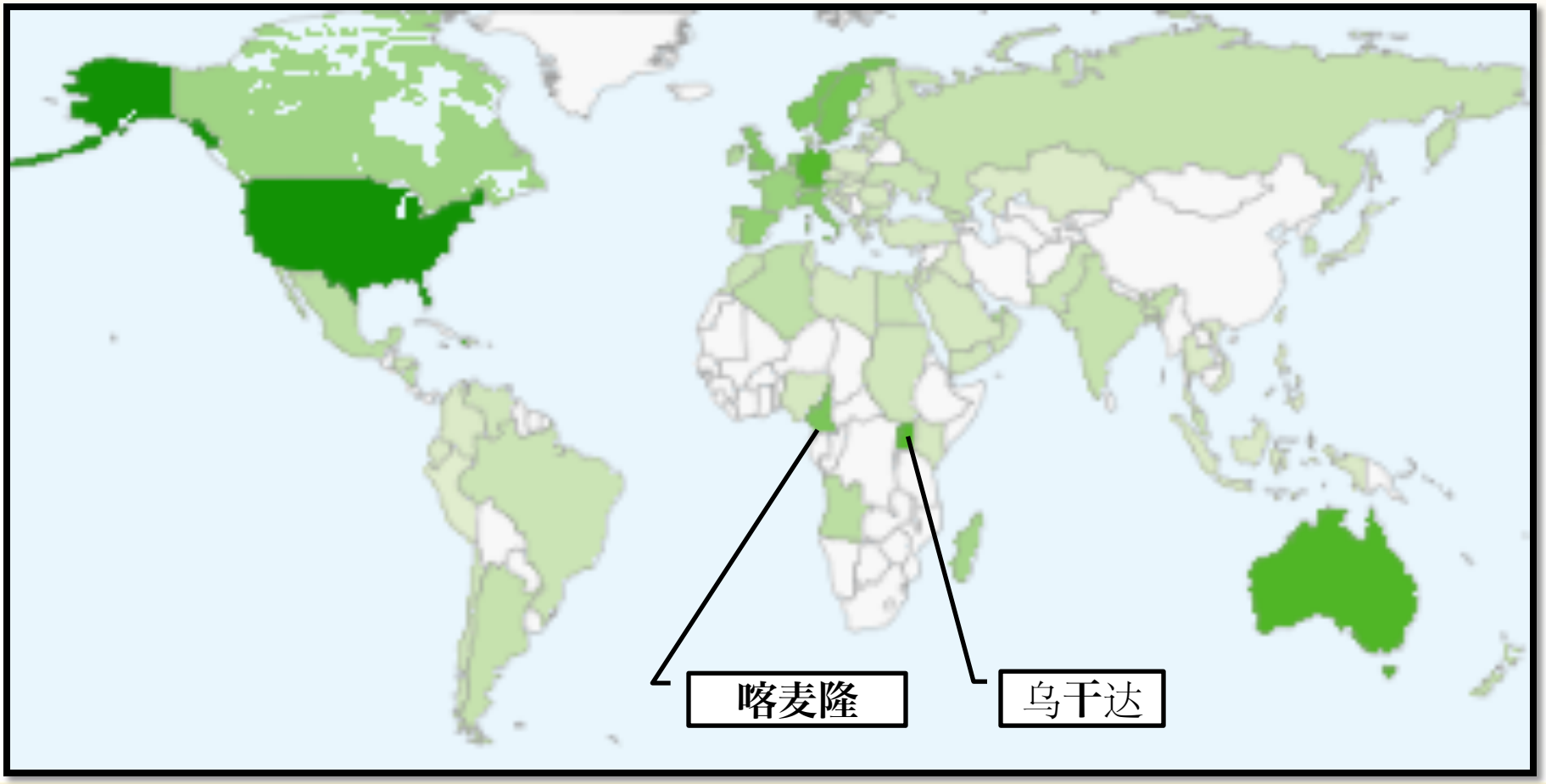


http://www.wired.co.uk/news/archive/2012-01/27/africa-twitter-traffic?utm_source=twitter&utm_medium=socialmedia&utm_campaign=twitterclickthru

flyingpenguin
the poetry of information security

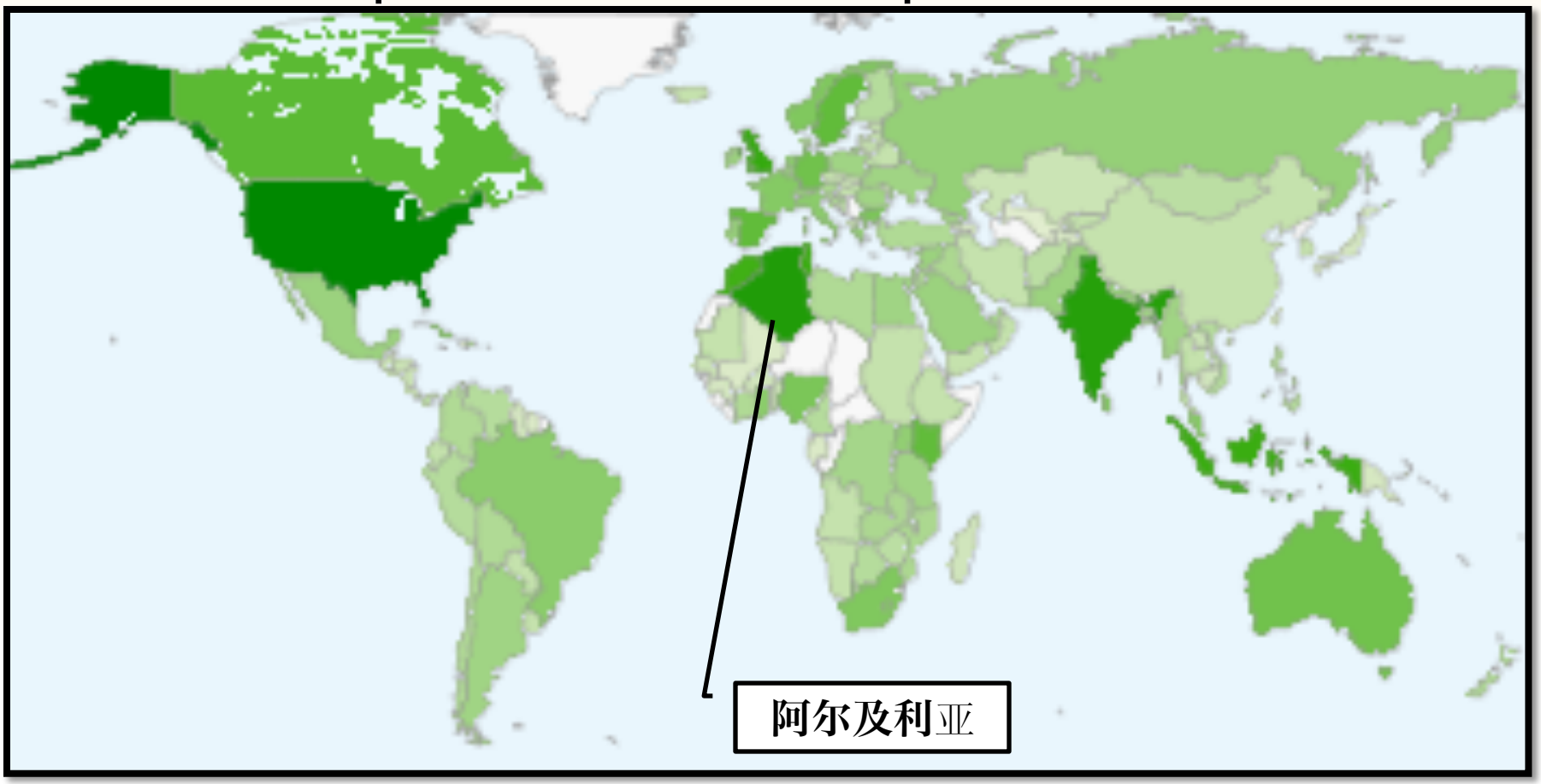
谁在培训什么？

- Black Hole RAT 教程



谁在培训什么？

- 使用 nmap nessus 和 metasploit 的黑客攻击



积极防御

- 监控（培训，工具包和工具）
- 发生异常时提醒（财富和资产）
- 基于数据采取行动

“[Koobface] 帮之所以取得成功，更多地是由于他们的不懈坚持以及不断进行调整的意愿，而不是技术完善性”

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

积极防御

1. 建立法律框架
2. 计算直接和附带损害
3. 声明目标和责任
4. 协作并收集数据
5. 积极防御

瓶中信：
在安全违规数据的
汪洋大海中寻找希望

DAVI OTTENHEIMER
FLYINGPENGUIN

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

会话 ID：
会话分类：