RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: CXO-R04

Lessons Learned From Real World CISOs

MODERATOR: **John Pescatore**
Director, Emerging Security Trends
SANS
@john_pescatore

PANELISTS:

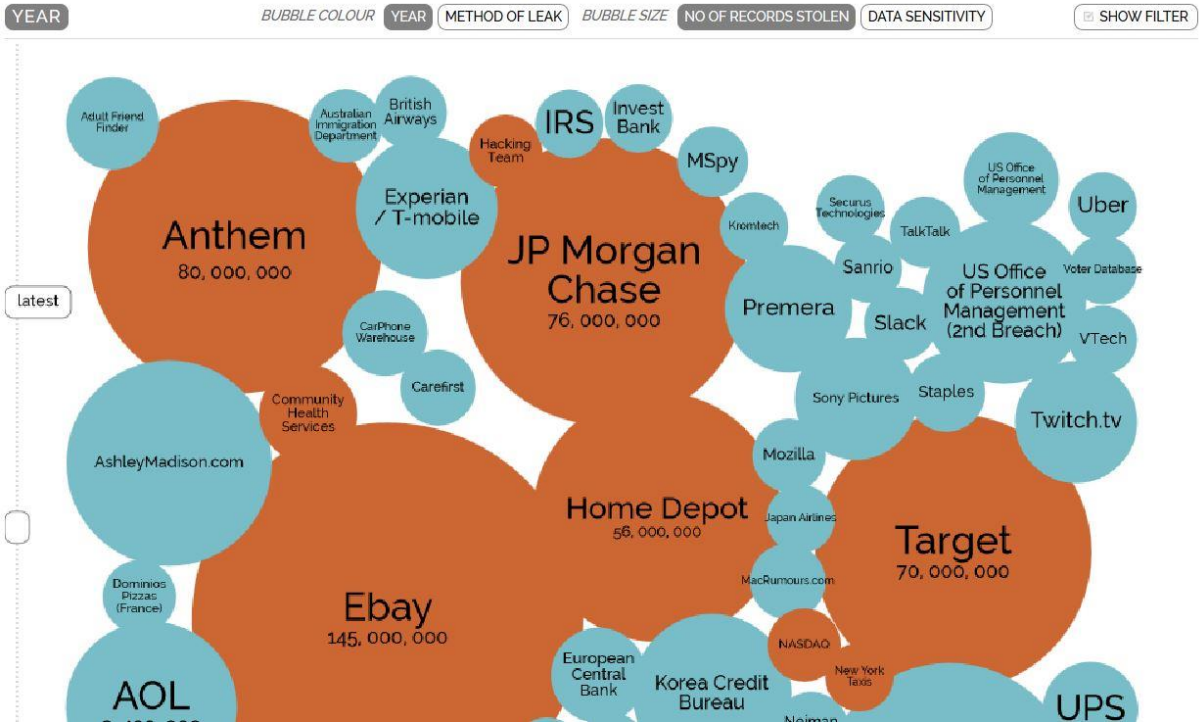
Tom Baltis
VP/CISO
Blue Cross Blue Shield Michigan

Randy Marchany
CISO
Virginia Tech

Pavel Slavin
Tech Director, Medical Device Security
Baxter Healthcare

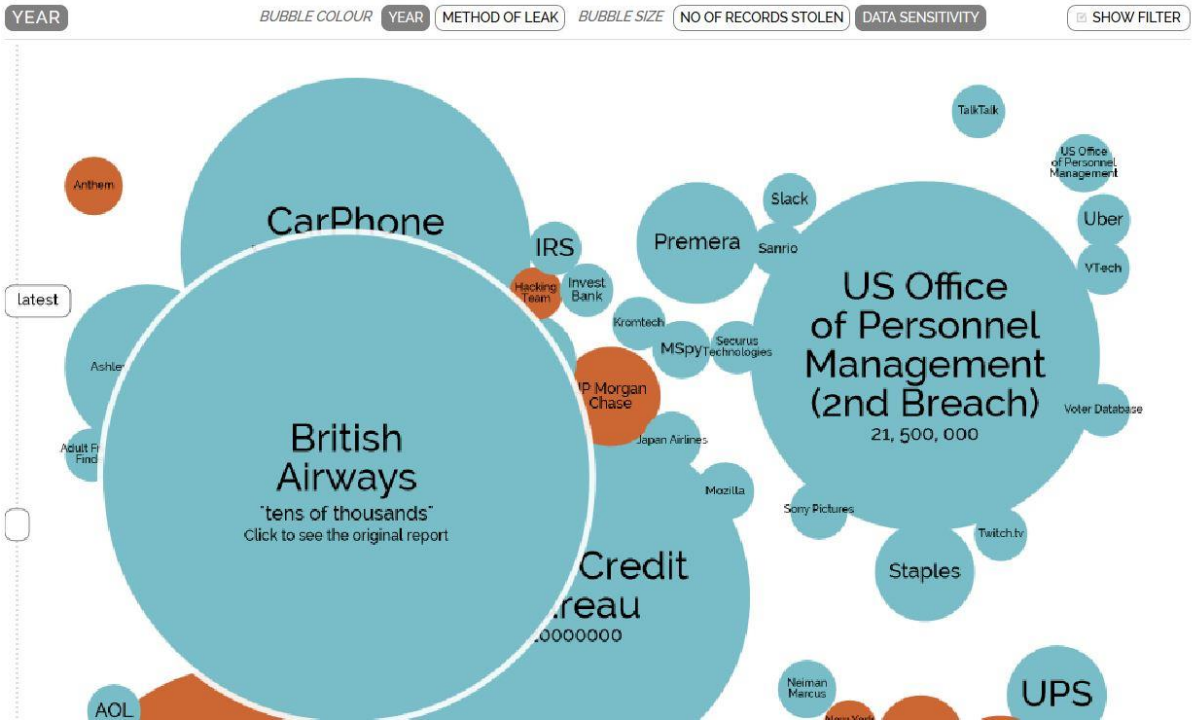
Don Smyczynski
CISO
Rich Products

Breaches Dominate the News – by size



Source: Informationisbeautiful.net

Business Impact Often Looks Different



Source: Informationisbeautiful.net

CISO Real World Hot Topics

- Balancing demands
  - Reduce threat impact to business
  - Reduce security impact to business
- Demands of particular industry/vertical
- Organizational drivers
- **Almost invariably, the organizations with the least cyber incident impact have the strongest CISOs and security teams.**

Learning from Real World CISOs

- I've asked each CISO to open with:
  - What are their top cybersecurity issues are for 2016 in their vertical, and how they plan to attack them.
  - What advice they have for the audience.
- We will then open up for audience questions. This is your opportunity to get specific and bring home information to apply when you get back.

Randy Marchany

CISO VA Tech

marchany@vt.edu

http://security.vt.edu

Who Am I?

- CISO at VA Tech
  - 40+K node network. dual stack IPV4, IPV6 network since 2005
  - Multi-national – Main campus (Blacksburg, VA), Remote campuses - NOVA
- My IT Security Philosophy
  - All Security is Local, all Monitoring is Central
  - The Business Process trumps the Security Process
  - Learn the business process before imposing security requirements
  - Restrictive security practices cause worse problems overall

It Takes a Team

VT Cyber Security Strategy

- University has 3 main business processes
  - Academic, Administrative, Research
- Academic
  - Open access needed – The ISP model
- Administrative
  - Traditional corporate security model
- Research
  - Hybrid
    - Open access
    - Restricted research, e.g. ITAR

VT Cyber Security Strategy

- BYOD
  - All students required to purchase their own computers, bring their own smartphones. We've been doing this since 1984
- The 20 Critical Controls are the foundation of VT cybersecurity strategy
- Security architecture must blend traditional corporate security with ISP security architecture
- Don't care what comes in, worry about what leaves the net
- Protect the sensitive data regardless of where it's located

RICH PRODUCTS CORPORATION

HEADQUARTERED IN BUFFALO, N.Y. SINCE 1945

BUSINESS SUMMARY

$3.5B
ANNUAL SALES

10,000+
ASSOCIATES

4,000+
PRODUCT CODES

36
GLOBAL MANUFACTURING FACILITIES

PRODUCTS

- Toppings & Icings
- Cakes & Desserts
- Pizza & Flatbreads
- Bakery Products
- Breads & Rolls
- Nut-Free Cookies
- Shrimp & Seafood
- Appetizers & Snacks
- Bar-B-Q
- Meatballs & Pasta
- Gluten-Free
- Syrups & Soaked Cakes
- Frozen Beverages

Global Food Manufacture Information Risk Management Program Profile

Don Smyczynski
Information risk management leader

- 5,000 knowledge workers operating in over 100 countries
- 36 discrete manufacturing plants in 10 different countries
- Federated IT / Security organization over 120 professionals supporting a common strategy
- Leverage Managed Services to scale program

2016 Top Five IT Security Concerns:

1. Theft of IP
2. Compromise of Industrial control systems
3. Breach of Energy management systems
4. The IoT wave
5. Management of Vendor access

Strategy to Address Top Concerns

1. Identify and prioritize risks, Implement controls, and continually test for compliance
2. Well-structured and tested data backup program
3. Isolate access and encrypt data
4. Privileged account management that incorporates a structured vendor management posture
5. Defined and adherence to standards
6. Audit for compliance
7. Segregation of the production network and office network

Lessons Learned/What Works

By three methods we may learn Wisdom:

1. By reflection, which is noblest

2. By imitation, which is easiest

3. By experience, which is the bitterest

Confucius