RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

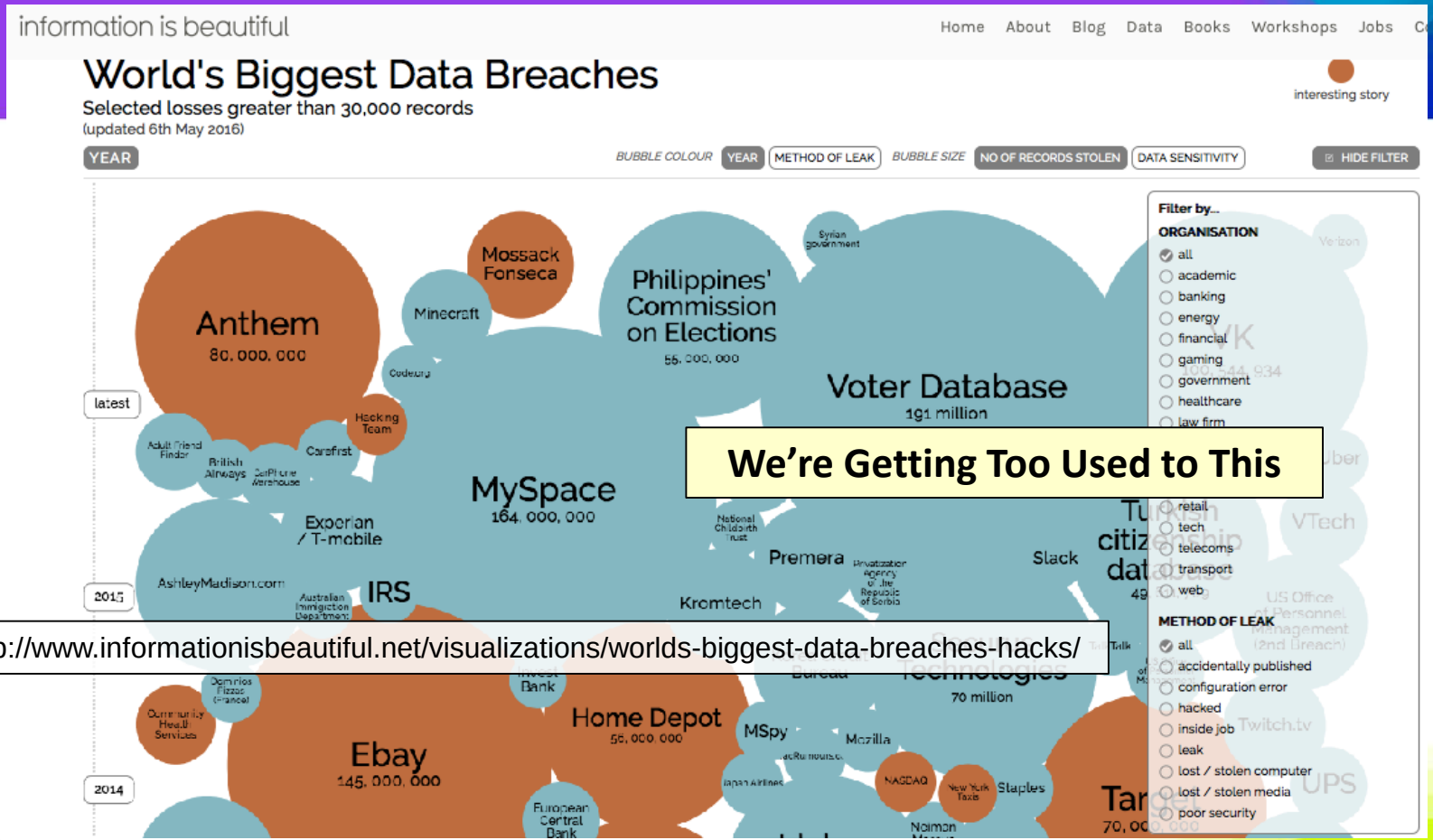
SESSION ID: STR-R10R

To Catch a Snowden

Addressing Insider Threat

Seizing [Back] the Initiative

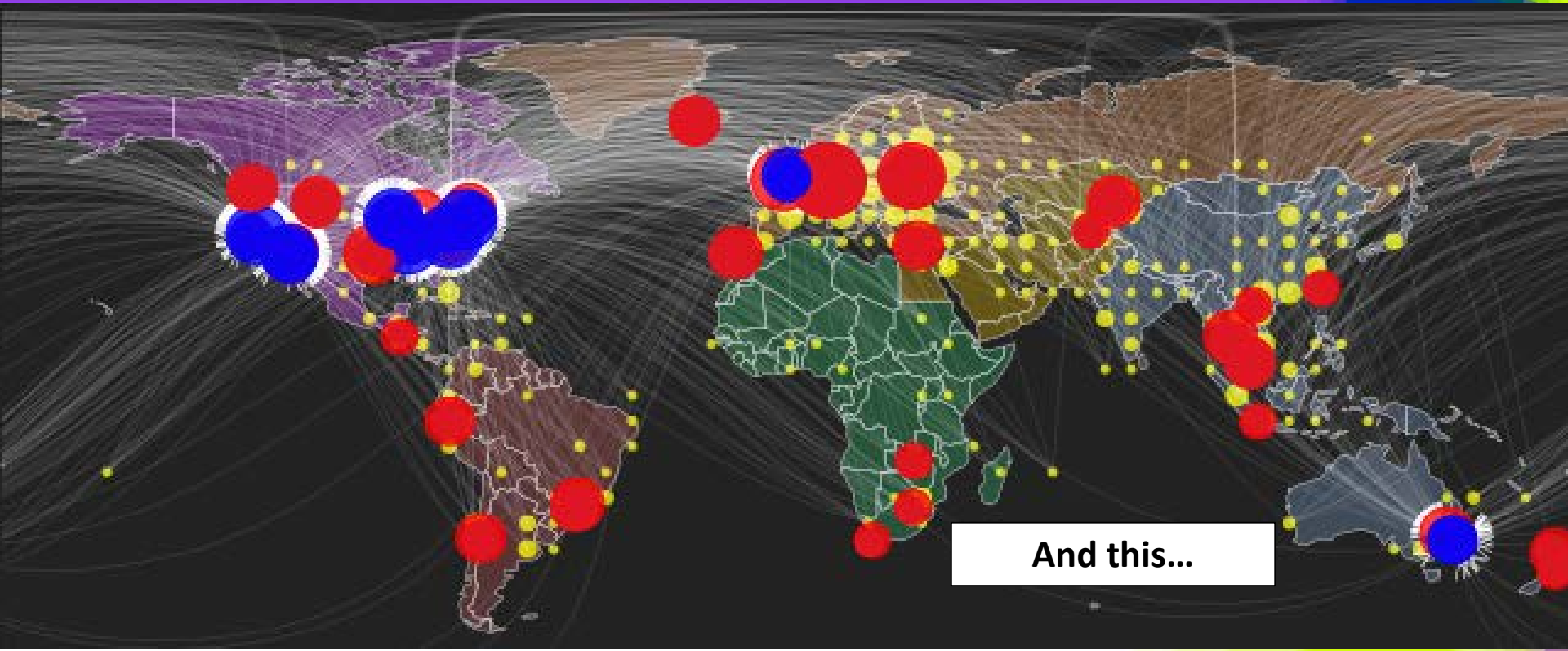
Chris Inglis
Advisory Board Chair
Securonix



We're Getting Too Used to This

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Everything's connected… A Day in 2013



Not to be outdone – there's the insider threat

Now in a theater near you…

Surveying the Cyber Landscape

Pockets of excellence exist *but* remain exceptional

Most organizations still:

Defend the wrong thing

… in the wrong time

Hold the wrong people accountable

… and worry about the wrong issues

First Principles - Three Things to Embrace

- "Cyber" is a Convergence of People, Technology and Process …
  … and Compels a Matched Response
  - *All **Three** Areas Must be Addressed … As a System*
- *Security* is not possible – *Defense* at net speed is the goal
  - *Defensible systems that are actually defended*
- It's About Operations … more than Technology
  - *Procedures, Cognizance, and Maneuver based on real-time cognizance*
  - *A word about Boards ….*

Behaviors transcend and give critical context to transactions

An Insider Threat Case Study

- **Strong application of *Protect* measures**
  - Hardware, software, doctrine
  - Driven by known or developing threats
- **Strong application of *Defend* measures**
  - Perimeter defense ***and*** defense in depth against external adversaries
- **Strong *vetting of insiders* to ensure trustworthiness**
  - Whole-person vetting to attain and sustain trustworthiness
  - Internal controls focused on coarse limits (allowing innovation and high rates o productivity)
  - Post-event analysis (auditing)
- **Expert Forensics , Feedback and Follow-up**
  - *If* an event is detected …
- **And yet… this was not enough. Why?**

Lessons Learned (Practitioner Level)

- **High speed, converged networks introduce high speed, high leverage vulnerabilities**
  - Defense has to operate “at user/network speed”
- **Network & operating system defense is NOT the sweet spot**
  - ***Move*** the focus to DATA … and do it in real-time
- **“Signature based defense” cannot keep up**
  - Understanding “behavior in context”… matters more
- **Culture remains the most powerful force in the world**

You cannot defend against ***some*** threats in real-time … and ***others*** in forensic time

Lessons Learned (Board Level)

- **"Harm" is exponentially higher and *different-in-kind* than a few yea**
  - Intellectual property theft at enormous scope and scale
  - "Reputation"
  - Attendant investment and opportunity costs
- **This is an *operational* – not a *technology* – issue**
- **There's no inside/outside anymore**
- **Stove-piped security across HR, IT, and Physical systems creates s**
  - **Connect them**
- **Culture matters … as much or more than technology**
- **Exercising for disaster is the prerequisite for success under fire**
  - Building muscle memory and intuition
  - Informing your investments
- **You can't go second in telling your story**
  - To customers, stakeholders, employees

Defend the Data – More than the Network
In Real Time, Based on Current Context

- **Segmentation, Privilege Management, 2 Factor Authentication improves defensibility**
  - While marrying convenience and security
- **Sensors, Tagging, and Analytics enable Cognizance and Action**
  - As close to real time as possible
  - *Behaviors* more than *signatures*
- **Leverage security analytics across enterprise initiatives**
  - Tip and queue across Information Technology, Human Resources and Physical security
- **Ensure protection of privacy through controls placed on use of user/adversary behaviors**
  - Privacy Protection Must be a ***Feature …*** US and European privacy schemes can be

Sensors (Data), Processing Power, and Analytics are Finally Ready to Deliver Real-time Cognizance

Summing Up

- **Assume adversaries are on your network**
  - Regardless of their physical location
- **Act on that assumption**
  - Instrument data, people, and sensors
  - Move from ***reacting*** well … to ***tracking*** well … to ***anticipating*** well
- **The paradox of defense:**
  - Allowing agility and respect for trusted parties while ….
  - Identifying and stopping inappropriate use, theft, destruction of corporate resources …
  - *At the speed of the stakeholders themselves*

Questions?