BUREAU OF THE
Fiscal Service
U.S. DEPARTMENT OF THE TREASURY

US Cyber Marathon

David Ambrose, Chief Security Officer and Chief Privacy Officer
Bureau of the Fiscal Service
U.S. Department of the Treasury

Context: US Government Scope/Scale

- 320M US citizens
- 4.1M Government employees (executive / military / legislative / judicial)
- 430+ bureaus/agencies
- 2,000+ data centers
- 95% of Internet traffic goes through a Trusted Internet Connection (TIC)
- ~$80B overall IT budget, ~$13B to improve cybersecurity (2015)

Recent Significant Cyber Breaches…

2014

- JPMorgan Chase: 76M customers
  - email, PII & credit card info
- Home Depot:
  - 56M credit cards & 53M email addresses
- Target: 70M customers
  - email, PII, and credit card info

2015

- Ashley Madison: 37M records
  - email, PII & credit card info
- Anthem Healthcare: 80M customers
  - PII
- Premera Blue Cross: 11M customers
  - medical records, PII, bank accounts

Total of 330M customers/records…

…..and now OPM (Office of Personnel Management)

June 2015

- OPM: 4.2M government employees
  - Payroll/PII data
- OPM: 21.5M government employees/contractors
  - 80M to 280M impacted when family/contacts/references included
  - Extremely sensitive personal & PII from background investigations

Government employee calculation:

Background investigation & payroll info (OPM) +

Medical info (Anthem or Premara) +

<u>PII & Credit card info (all other breaches)</u>

= *Comprehensively breached government employee*

Cybersecurity Sprint

- 30 days - June 12 to July 12
- Objectives:
  1. Scan for "indicators of compromise" listed in the U.S. Computer Emergency Readiness Team's Analysis Report
  2. Patch critical vulnerabilities
  3. Tighten policy and practices for privileged users; minimizing number and limiting the functions
  4. Accelerate implementation of multifactor authentication
     - Priority on privileged users
  5. Identify and catalog high-value data, systems, equipment, infrastructure and applications
     - Make a risk-based assessment of current cybersecurity and physical security protections for those items

Cybersecurity Marathon goals

- Identify
  - High value assets
- Protect
  - Credentialing, vulnerabilities
- Detect
  - Analytics, network traffic
- Respond
  - Standards, improved timelines
- Recover
  - Standards

- Address Human Resource issues
  - Map and optimize cyber staff
- Plan for emerging technologies
  - Incubate & adopt

We still have a long way to go

- Majority of agencies still non-compliant with the 10 core FISMA requirements
- Roughly half of federal agencies continue to report ongoing cybersecurity weaknesses in all five federal categories
  - Spend: about $91B on FISMA investments over the past eight fiscal years
  - $12B in FY 2014
  - 22 of the 24 major agencies report material weaknesses in three categories: access control, configuration management, and security management.

Federal Cybersecurity Policy Lacks Focus

- As of fiscal year 2015, Government Accounting Office (GAO) reported a total of 62 separate federal cybersecurity centers
- New, often overlapping legislation developed every few years:
  - **1998**: Presidential Decision Directive 63 (PDD-63) strove to "eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures"
  - **2000**: The National Plan for Infrastructure Protection (NIPP) defined "critical infrastructure assets"
  - **2002**: The Federal Information Security Management Act (FISMA) defined milestones and investments in information security systems to be completed by 2010
  - **2003**: The National Strategy to Secure Cyberspace prioritized cybersecurity threat identification, response, and notification

Federal Cybersecurity Policy Lacks Focus

- **2008**: The Comprehensive National Cybersecurity Initiative (CNCI) outlined a cybersecurity strategy emphasizing threat detection and information sharing
- **2009**: Cyberspace Policy Review initiated to try to unify policies and promote sharing of cybersecurity information among public and private groups
- **2013**: Executive Order for National Institute of Standards and Technology (NIST) to develop a “Cybersecurity Framework” for critical infrastructure assets
- **2014**: National Cybersecurity Communications Integration Center (NCCIC) defined as the main federal cyber information sharing hub; FISMA amended

Legal Environment

- Case law has not caught up with current environment
  - For example, existing case law is interpreted to forbid a company from entering another network to delete its own data
  - Case law on physical assets is being interpreted differently for virtual assets (i.e. cybersecurity)
    - No consensus yet in international law

- Again, new laws being proposed this year:
  - The Consumer Privacy Protection Act of 2015
    - Protect PII and reporting of breaches
  - Cybersecurity Information Sharing Act
    - Federal/private information sharing
  - Federal Information Security Management Reform Act
    - Strengthens the ability of the Secretary of Homeland Security to detect and prevent intrusions against, *and to use countermeasures to protect*, Government agency information systems

Sprint/Marathon Lessons Learned

- It’s not just PII & industrial espionage
- Legislative focus needed
- Invest in training – people link still weakest
- Legal issues cross borders
- Breach impacts moving from virtual to physical…..spies, cars, Internet of things
- Need rules for fighting back
  - Three A’s: annoyance, attribution, attack
- Adversaries have very long timeframes

Contact Information

Primary Contact

David Ambrose
Chief Security Officer
Chief Privacy Officer
202-874-6488
David.Ambrose@fiscal.treasury.gov