Cyber Security: The World at a Crossroads

RALPH R RUSSO
TULANE UNIVERSITY
SEPTEMBER, 2016

Agenda

I. THE THREAT/RISK
II. THE CHALLENGES
III. THE RESPONSE

The Threat: What Is Everyone So Excited About?

THINK MAJOR RISK TO:

FREEDOM, PRIVACY, CIVIL LIBERTIES, FREE ELECTIONS, HOMELAND SECURITY, INNOVATION/INTELLECTUAL PROPERTY, COMMERCIAL / BUSINESS VIABILITY, SUPPLY CHAIN, US WORLD STANDING, HEALTH, ELECTRICAL POWER, BANKING, ETC

The Scope/Severity of the Problem: IP

Innovation and R&D viability in an insecure cyber world

Why would one company/country spend $$$$ to innovate, when another can steal the IP and produce copies for almost nothing

Scanners, shredders, electrical plugs that steal

THE WALL STREET JOURNAL.

http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003

OPINION | COMMENTARY

Protecting U.S. Innovation From Cyberthreats

Our new national action plan includes $3 billion to kick-start an overhaul of federal computer systems.

By **BARACK OBAMA**

Updated Feb. 9, 2016 5:14 a.m. ET

More than any other nation, America is defined by the spirit of innovation, and our dominance in the digital world gives us a competitive advantage in the global economy. However, our advantage is threatened by foreign governments, criminals and lone actors who are targeting our computer networks, stealing trade secrets from American companies and violating the privacy of the American people.

Networks that control critical infrastructure, like power grids and financial systems, are being probed for vulnerabilities. The federal government has been repeatedly targeted by cyber criminals, including the intrusion last year into the Office of Personnel

The Players: Matthew Broderick to Big Time

- Hackers have Evolved: Now Nation-States and Vast Cyber Criminal Enterprises
- Hacker Goals have evolved: From ego-driven on small scale to Malicious intent on grand scale
- Skill-level required to achieve goals has been lessened
  - Attack tools and "tutorials" freely available on cyber underground
- Attack Targeting is evolving
  - From Wide-net indiscriminate methods (phishing), to complex and sophisticated, targeted attacks (Advanced Persistent Threats, Polymorphous/Modular attack malware)
- Cyber Attacks are clearly the Future:
  - Getting easier, allows anonymity, much more lucrative, significantly lower probability of being caught, low risk of harm to attacker

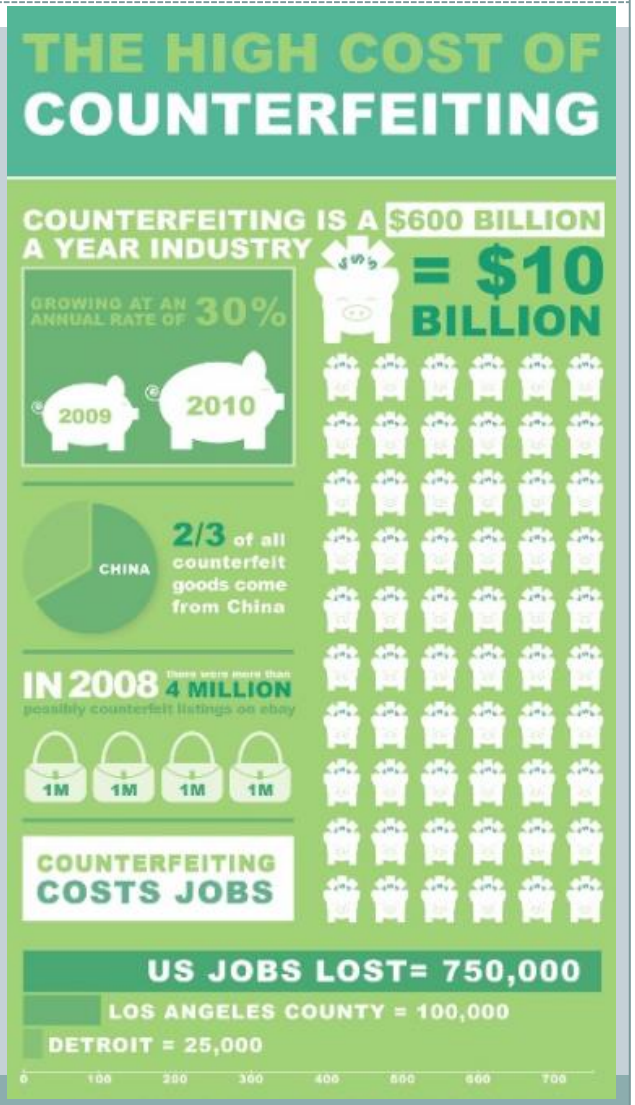
Why does this evolution present a risk?

- Cyber Networks, Data Structures and Software as society foundation like steel, cement, electric, gas engine, medical practice
- Fully dependent on Cyber: Consider:
  - Supply Chain, Refineries, Electrical Grid
- The difference is that development of other Foundation-level systems and tech were subject to rigorous levels of process for safety/security by credentialed, educated practitioners (engineers, doctors) learned in the best practices and leveraging a common standard.
  - "Basement" companies: Technology/Applications/Networks built by people without a base-level common standard, standard of education
- No incentive for software companies to bake in security

See "Geekonomics" by D. Rice

What is the Worldwide Power Structure Risk?

- Game-Changer that will reshuffle the Power structure amongst nations, change economies (Cyber Crime), warfighting (Cyber War).
  - Intellectual Property and technologies from US R&D, Safety protocols, and cutting edge development is being stolen at unprecedented levels.
  - Counterfeiting is costing US jobs (and the taxes from workers and sales) to the tune of 750K jobs and $10B a year. China is responsible for 50% of the World's counterfeit goods
  - Kinetic war without Cyber Component is a thing of the past.
- Cyber Attacks evolving as a war/terror tool



http://www.ritholtz.com/blog/2011/07/the-cost-of-counterfeiting/
http://www.businessinsider.com/15-facts-about-china-that-will-blow-your-mind-2010-2?op=1

The Misalignment and the Challenges

Advanced Persistent Threats

- APT: Game Changer:
  - StuxNet (Iranian Nuclear Program), Flame, Duqu
- You say you want an Evolution?
  - Citizenry struggling with technical concepts
  - Difficult challenge as classic political elements of Privacy, Civil Liberties, Government involvement are at the center of the issue.
  - Political infighting and posturing, while nation risks “digital pearl harbor” or erosion of our status in the world

How about Privacy & Civil Liberties?

- Huge Risk as laws, policies are crafted
- Laws written to interdict cyber crime could be used in ways that stifle free speech, and other freedoms
- Computers are tools, and tools that are evolving much faster than regulatory cycles.

OPINION: Existing criminal laws should be applied in most cases, with the cyber element viewed as weapon, methods or means to a traditional crime

We are using old concepts to try to describe a new paradigm

- International? Domestic? Does not apply in terms of threat actors
- Government “Lanes”: MIL | FCI| Local LE | Secret Service | DHS - Do not apply to the Cyber Threat
- Positive, 100% attribution: almost impossible without admissions
- Traditional “Lanes” of protection (Military external threats, Law Enf/FBI criminal threat etc.) do not fit the Cyber Threat matrix
  - Same Actors may work across Cyber War, Cyber Terror, Cyber Crime, Hacktivist threat types

BIG FAIL: IT as a separate, and lesser entity in almost all Commercial and Gov. Entities

- Cyber Security is the job of the CEO, not a lesser position
- All Executive Leadership must, therefore "bake" in Cyber Security as part of any and all initiatives including Finance, Accounting, Marketing, R&D, Manufacturing
- "CIO" = Career is Over

Our Current Cyber Security Posture

- We do not plan to fail, yet we fail consistently
  - Vulnerable: No "connected" system is 100% invulnerable to attack
  - Anti-Virus/Spyware/Firewalls vulnerable to Zero Day attacks
- The flip side: "Over" Secure posture leads to massive insecurity problems

The Response: Where do we go from here?

What can we do?

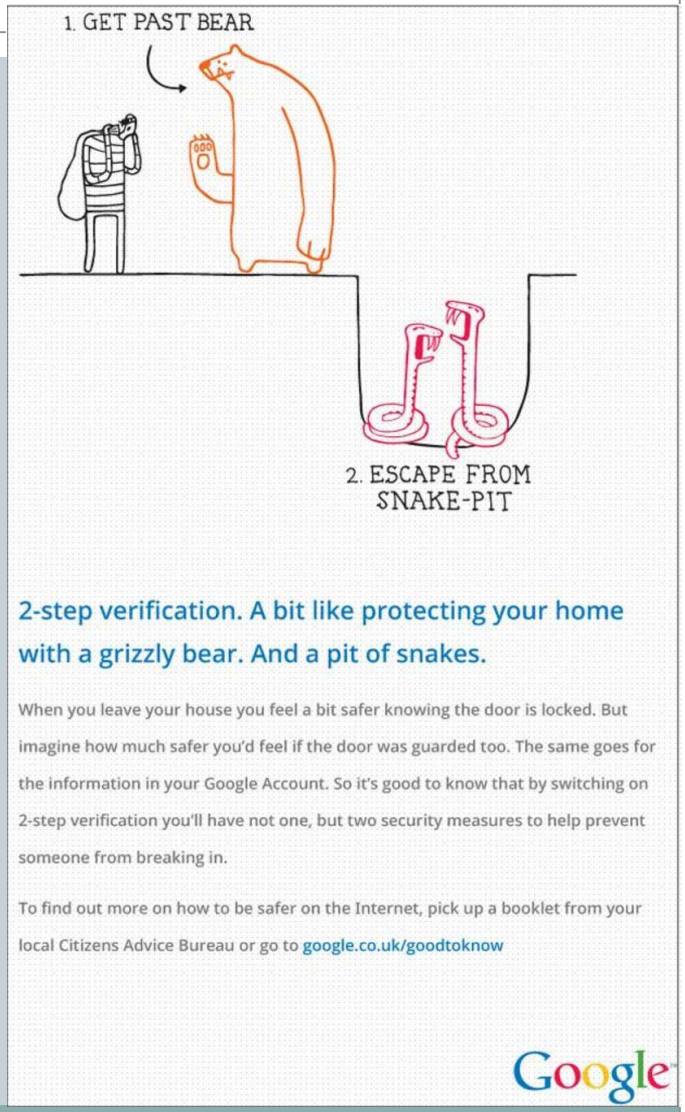
- Government as facilitator, providing framework, goals, structure, process, best practice, funding to incentivize cyber security goals
  - Not regulate-first
- IT and Cyber Security as the CEO's job
- Need specificity in National Plan, and National framework built to achieve stated goals
- Need to structure security posture and responsibility to the threat, not to traditional "lanes"
- Need structure to collect and share intelligence and information (trends) across commercial, government, citizenry while not adversely impacting commercial competition

What can we do? (pt. 2)

- Need standards for systems security, ratings for software re: security
  - Simplify: Need tailored best practices that are shared in a brief, understandable fashion. Updated frequently.
  - Simplify: If you can't document your network, you can't secure your network
- Understand where to segregate your network (subnets) – "need to know" for network access
- Need to promote, drive Risk Management for small/medium businesses
- Need everyone in the game: Software/DB developers, ISPs, end-users(!)

Example: simple communication for unsophisticated users

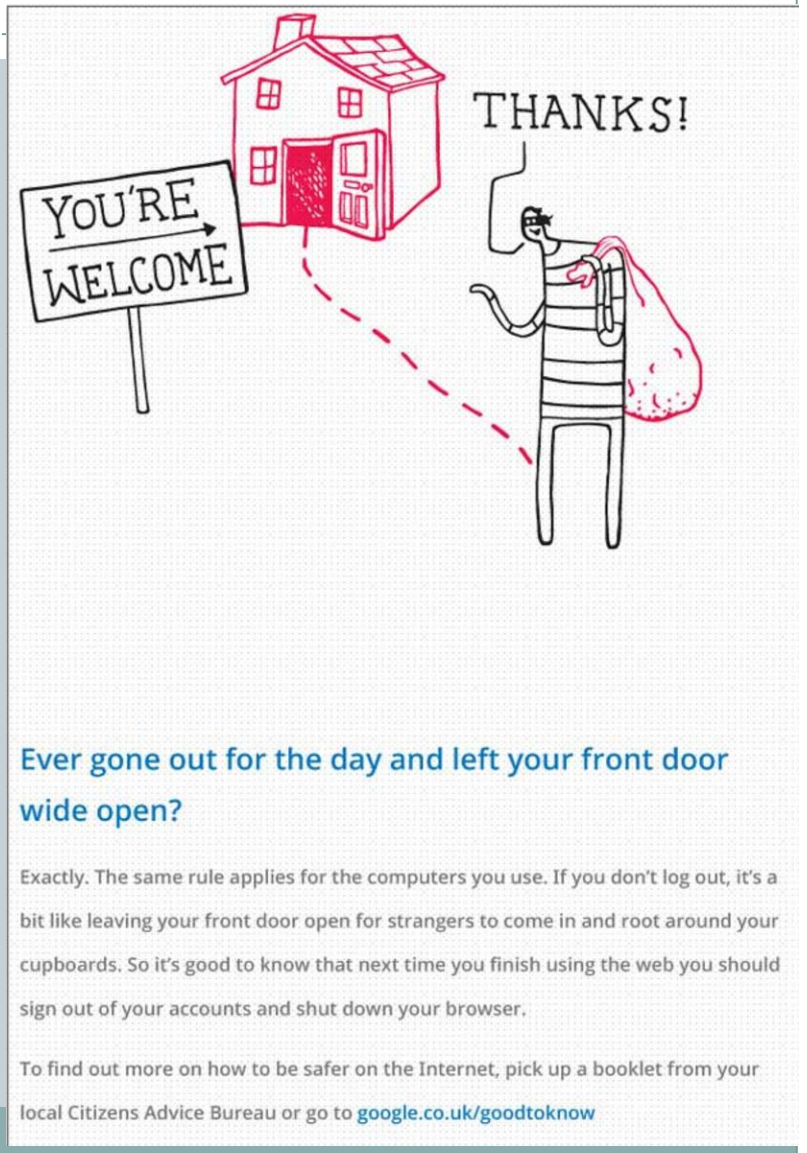
- What is a $10,000 door with a $2 lock worth?
- US spends more than $12B a year* on Cyber Security, considered “not enough”
- However “best practices” are complex, and have almost zero penetration to the end user. Compare that to Spear Phishing and Social Engineering problems
- Compare to Google “Good to Know” Campaign



*http://www.businessinsider.com/us-government-cybersecurity-spending-2015-9

Action Example: Align education and response to Physical Security Concepts

- Consistently Fail to achieve longstanding Security Goals:
  - Defense in Depth,
  - Separation,
  - Deception,
  - Diversity/Commonality,
  - Discretion,
  - Collection,
  - Awareness,
  - Response



Cyber Security and Auditing

- Auditing: Critical Role
- Alphabet Soup without coherence: SOX, FISMA, Red Flags, GLBA, PCI DSS, HIPAA, PCAOB, CIPA etc
- Auditor = Listener….
- Holistic: Concentrate on Concepts, not ever-changing technologies
- How clear are Best Practices made to Employees? Fire-hose versus Clear message including reasoning
- End-point security: Computers locked? Sharing Passwords? Written down passwords?
  - Watch for “Over” Secure, work-inhibiting posture driving insecure workarounds

Questions/Resources?

- Resources:
  - NIST Cyber Security Framework
  - NIST Security Handling Incident Guide
  - US Secret Service Best Practices for Seizing Digital Evidence
  - Google “Good to Know” Program
  - US National Strategy to Secure Cyberspace
  - US Cyberspace Policy Review
  - US National Strategy for the Protection of Critical Infrastructure
  - US National Military Strategy for Cyber Operations
- Sources and Further Reading:
  - Future Crimes: Marc Goodman (Trends, Risk, Great Real-world application)
  - Cyber War: Richard A Clarke (Global, Risk)
  - Geekonomics: David Rice (The Problem)
  - Cyber Attacks: Protecting National Infrastructure: Edward Amoroso (Concepts for Solutions)
  - CyberPower and National Security: Kramer, Starr, Wentz (Wide Scope, Deep Dive)
  - The Next War Zone: James Dunnigan (Older, Prescient)
  - The Cuckoo's Egg: Cliff Stoll (Fun Read, Old)
- Ralph Russo
  - rrusso@tulane.edu
  - Follow me on twitter: Daily Cyber Security and HMLS tweets: @rrhmls