Cybersecurity in a Global Economy

Matt Morton
CGEIT, CISSP
Do we really need cybersecurity?
Linked Globally
Office of Personnel Management

• 25 million affected
  • Security clearances
  • 2.1 million fingerprints
    • Wait - 5.6 million
• Upgrading systems since 2010
• Too little too late
• Incremental contracting
• Political favors
• Government shutdowns
New Approaches
Ideas
Stealing Ideas
“We have always been shameless about stealing great ideas.”

Triumph of the Nerds (1996)

Steve Jobs, 1996.
Temüjin

- Organizing tribes
- Common goal
  - Prosperity for all
    - At least those who submit
- Controlled all commerce for 3 centuries
- From Poland to Korean coast
- Cultural impact reaches into current times
- Who is this?
Chingis (Genghis) Khan

- Dominated all of Eurasia
- Conquered Russia
  - China
  - Eastern Europe
  - Middle East
- Multiple contributions
  - Military strategy
  - Multiple cultures within one empire
  - Religious tolerance
  - Trans continental mail system
  - Paper money backed by precious metals
Mongolian Global Economy

• Controlled all commerce well into 14th century
• Encouraged safe, fast communication throughout empire
• No real desire to manage countries
• Control of mail riders
  • Ability to intercept
  • Read messages
• Seeing a pattern?
What’s different today?

• Similar battle today in dealing with Mongolian strategy
• Multiple tribes or groups on the Internet
• Freedom of expression on Internet
• Continued attempts to extract tribute
Ransomware
Phishing
Cybercrime Hierarchy
Coalescing Groups
Interconnected
Hacking the Telegraph

Swift and Sure.

Since justice took to tracking crime by the aid of the Electric "Pude pone cludo." No wonder the murderer is nervous, when he is, Telegraph, she can no longer be described in the words of Horace as, literally, very often "hung upon wires."
Hacking Wireless Telegraph
Projector hacked by Maskelyne
Zimmerman Telegram

• Sent by Germans in 1917 to Mexico
• Sent from German Embassy in US
• Intercepted by British Intelligence
• Decrypted and shared with U.S.
Phone Phreaking
Arpanet Computer
New York (TheStreet) -- Bitcoin has existed in a zero-interest rate environment since its introduction, but that may be about to change. And if and when it does, the digital currency will feel the impact.

The Federal Open Market Committee (FOMC) will vote this week whether to raise the benchmark interest rate from the 0.25% it has been set at since December 2008. While most analysts believe this week’s meeting won’t bring a rate hike, they concur that it will likely happen by the end of the year.

The latest dot plot released in the FOMC’s summary of economic projections in June

Stock Watch

3 Stocks Carl Icahn Is Buying in 2016
5 Hated Earnings Stocks You Should Love
7 Health Care Stocks John Paulson Is Betting On in 2015

Call Up Some Big Gains With These 5 Telco Trades
VKontaoke
Qzone
Odnoklassniki
Darkode

This domain and website have been seized by the Federal Bureau of Investigation, Pittsburgh Field Office and the United States Attorney’s Office for the Western District of Pennsylvania as part of a joint law enforcement operation by the F.B.I. and international law enforcement agencies acting through Europol.
Silk Road
APT1
Lizard Squad

#OFFLINE
Chelsea Manning
Snowden
2014

• 312 breaches
  • Up from 253 in 2013

• 1.1 million identities exposed on average

• Top three sectors
  • Healthcare
  • Retail
  • Higher education
Yikes!

- Average cost of breach
  - $217 per record
- Average organizational cost
  - $6.53 million
- Higher Education average cost
  - $300 per record
  - 150,000 identities
    - $45 million in direct and indirect costs
What happens to those that deal poorly?
MCCCD EMPLOYEES: BREACH WARNINGS IGNORED
DISTRICT SAYS WORKERS WITHHELD INFORMATION
Maricopa

• Multiple breaches
• Board refused to fix issues
  • Political battles
• 2 class action lawsuits
  • Average compensatory damage request
    • $3000 per claimant
  • 2.5 million identities
  • Maximum claim of $15 billion dollars
  • There is a cap
• 2 FTC complaints
Do we care?

- 76% of citizens surveyed said they felt stress as a result of being notified
- 57% of consumers said they would discontinue or be less likely to continue a relationship with a company that lost their info
- On average 6% “churn” rate
- Do we follow through with these sentiments?
11 Worst Breaches of all time

- Heartland Payment Systems, 2008-2009: 130 million records compromised
- Target Stores, 2013: 110 million records compromised
- Sony online entertainment services, 2011: 102 million records compromised
- National Archive and Records Administration, 2008: 76 million records compromised
- Anthem, 2015: 69 million to 80 million records compromised
- Epsilon, 2011: 60 million to 250 million records compromised
- Home Depot, 2014: 56 million payment cards compromised
- Evernote, 2013: More than 50 million records compromised
- Living Social, 2013: More than 50 million records compromised
- TJX Companies Inc., 2006-2007: At least 46 million records compromised
- LastPass – 2013, 2015 – multiple computer password hashes lost
Sony Pictures

HACKED
Sony Pictures

• Perpetrated by Lizard Squad (as GOP)
• May have been hired by North Korea (Schneir)
• Paid fired Sony system administrators for inside information
• FBI investigation continues
• Will cost Sony 35 million to repair holes
• Although no bottom line impact it remains to be seen if the brand damage will prevent talent from working on Sony pictures.
• Began with phishing attack to iPhones
Target
**Step 1**
Target installs $1.6 million malware detection from FireEye, the detection service used by the CIA and other intelligence agencies.

**Step 2**
Hackers gain access to Target’s network through a third party vendor -- a HVAC company from PA.

**Step 3**
Hackers sent malware to skim credit card information from point of sale terminals at all US Target stores.

**Step 4**
November 30 - FireEye systems sound alarm to Bangalore team which notifies Target security team in Minneapolis. Target missed these.

**Step 5**
December 2 - Hackers installed another version of the malware and credit card information starts pouring out. Again, FireEye and Target systems noticed the breach, but company did not act.

**Step 6**
Hackers needed a way to get credit card data out of Target’s systems and onto their own. They set up three "staging point" servers in the US before.

**Step 7**
December 12 - DOJ notified Target about the breach. Target’s investigators go back and notice that their alarm systems went off twice during the breach.

**Step 8**
December 15 - Target eliminates the malware after 40 million credit card numbers were taken.
Target

- Began as an intrusion from a third party vendor system to work on their HVAC system
- Compromised the POS terminal at all of their stores
- Target systems detected intrusion within an hour of it occurring
- Team in India notified the team in Minneapolis
- more than 2 weeks before they were actually responding to it but by then it was too late.
Damage

• 40 million credit and debit cards numbers
• 46% drop in profit in the 4th quarter of 2013
• Cost to bank and credit unions to reissue cards - 200 million dollars
• 100 million to upgrade all terminals
• Class action lawsuit - 10 million
• Total cost in excess of 1 billion dollars
• Now Target has laid off 13 percent of its workforce in the 1st quarter of 2015
Wait . . .

- 46% drop in profit
- Stock price drops to 1/2 of its original trading price (it has since rebounded)
- CEO - gone
- CIO - gone as well as a large amount of mid level managers
- And now laying off 13% of its workforce?
- Probably not their business objectives
Root Cause?

• Definition of business value
• My definition
  • Balance of governance and growth
• Profits only mindset
  • Leaving support activities unfunded or understaffed
• Government and non-profits
  • Value is being defined as cost reduction only
  • Not in the quality of services
What can you do?

• Don’t use personal information when it’s not necessary.
• Keep a list of who has your data
• Use secure passwords
• Encryption is good 😊
• Make sure and lock down your WiFi
• Ask questions of those who want your personal info
What can you do?

• When in doubt throw it out - Data Privacy Day – Jan 28th
• Report any problems/concerns to www.ic3.gov
• Backup your important data
• Be careful using public hotspots - limit what you do on those sites
• Strong passwords
• Use a good Antivirus solution - many are available for free
• Phishing
What can we all do?

- Talk to your local representatives
- Talk with your business
- Be an advocate in the community
- Participate in Cyber Security Awareness Month Oct
Education

• Cyber security literacy in elementary school through college
• All empowered leads to more difficult to fool
Board Visibility

• Take Cyber Threat seriously
• All boards
  • Profit
  • Non-profit
  • Educational
• Recognize the cost of assuming risk
Law Enforcement Support

• Need tools to do their job
• They DO NOT need shortcuts that sacrifice our privacy
Collaboration

- Threat is shared
- Bad guys exploit our
  - own selfish self interests
  - Siloes
  - Bureaucracy
- Cost should be shared
- Information needs to be able to assist without creating jeopardy
Mongol Success

- City states were isolated and didn't work together
  - Fewer numbers
  - Less resources
- Mongols in Eastern Europe
- Keys to winning
Finally

• Collaboration is key
• Transparency
• Amplify the effect of our resources
• Develop sharing methods
• Secrecy can be used against us
• Trust across all sectors
Questions?

• Thank You!