Cybersecurity Challenges Facing Today's C-Suite: An Inside Look With the FBI

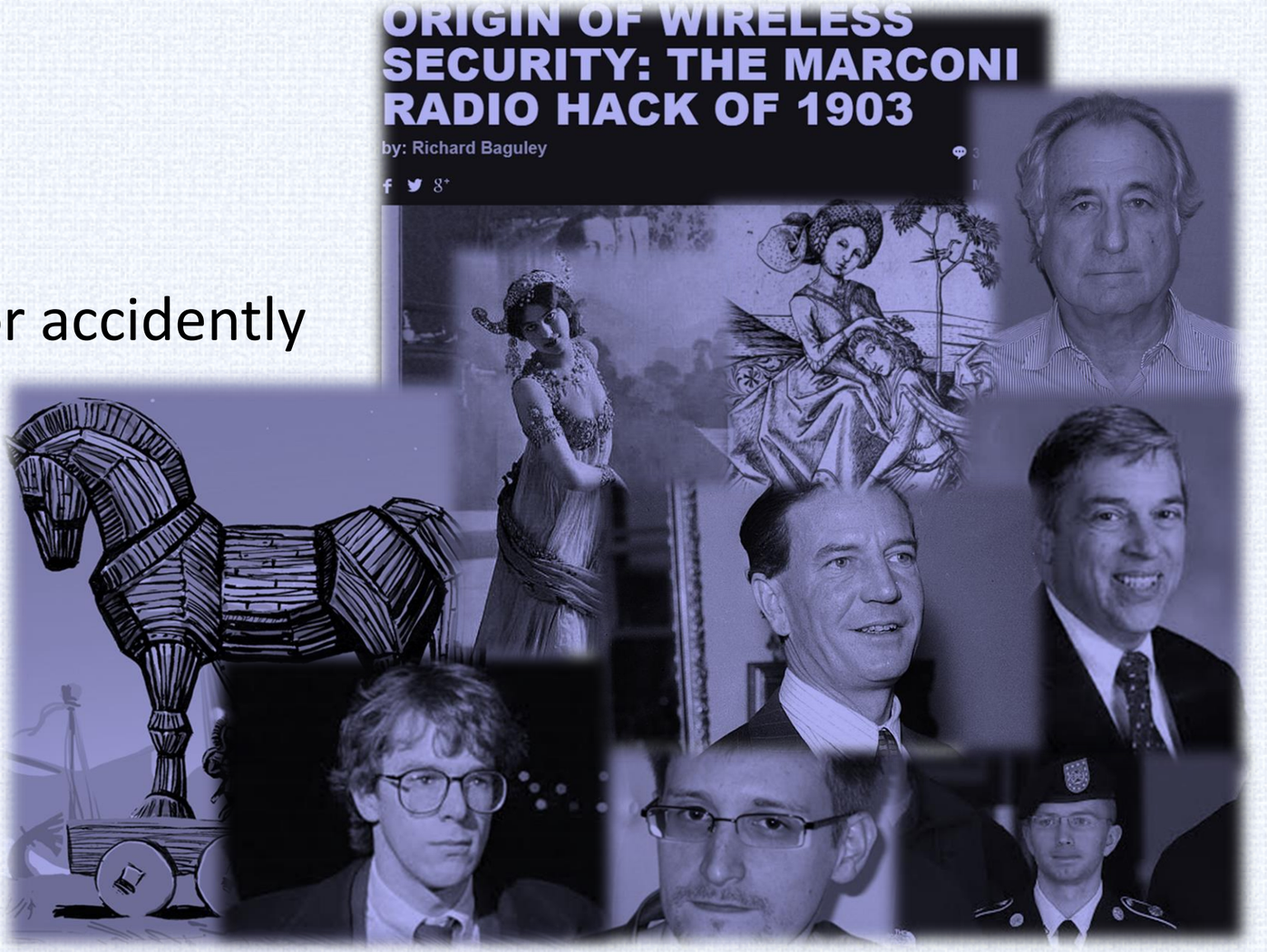
Arlette Hart

Federal Bureau of Investigation

Everything Old is New Again

https://hackaday.com/2017/03/02/great-hacks-of-history-the-marconi-radio-hack-1903/#more-245251

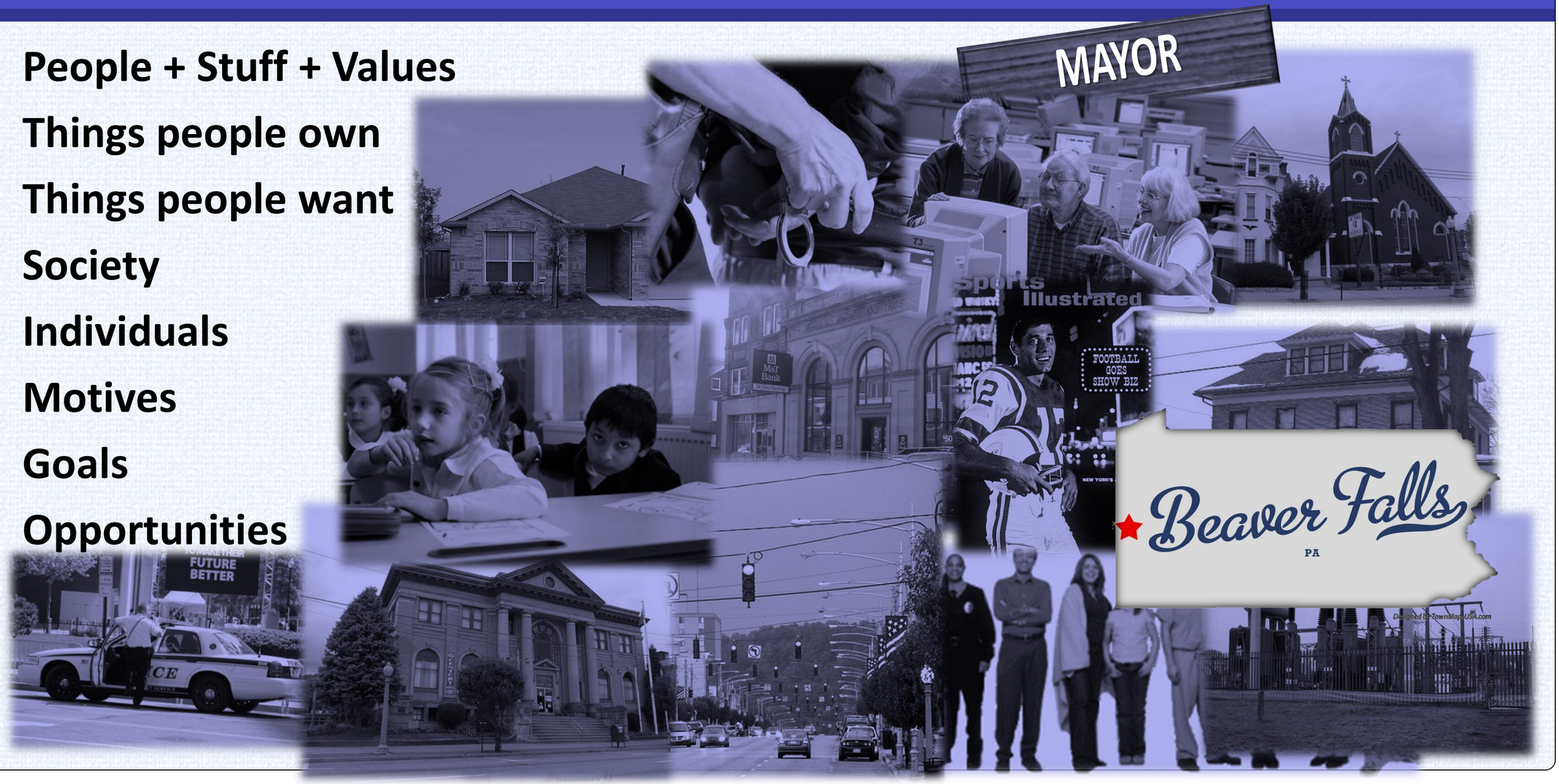
- Started when people started
- People attack from the outside
- People steal from inside
- People deceive – intentionally or accidently and they try to cover it up or escape consequences
- It's easier to compromise from the inside – except you have to hide more.



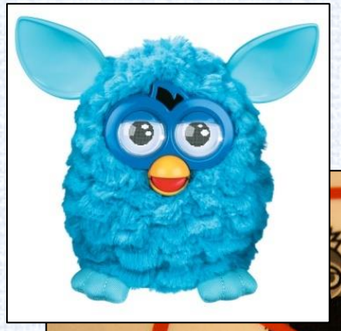
People change; People's motivations change

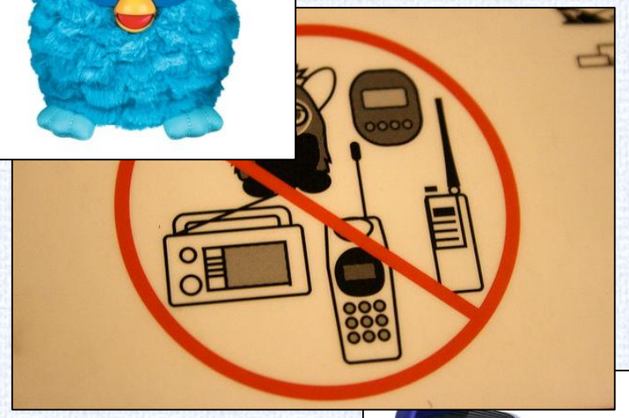
The Landscape

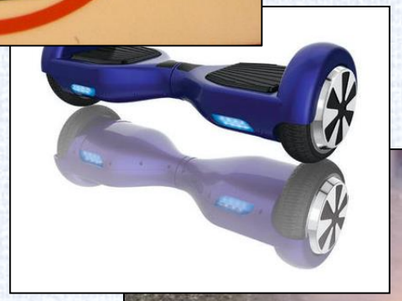
- People + Stuff + Values
- Things people own
- Things people want
- Society
- Individuals
- Motives
- Goals
- Opportunities

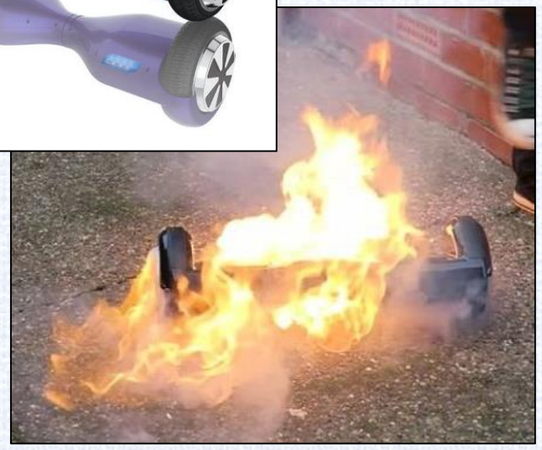


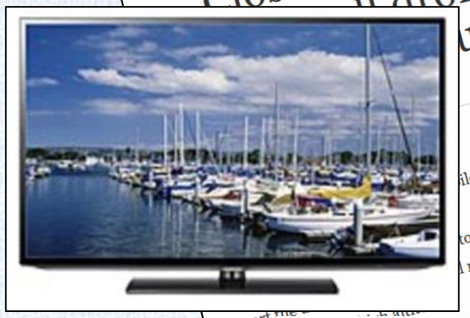
When Toys Attack …

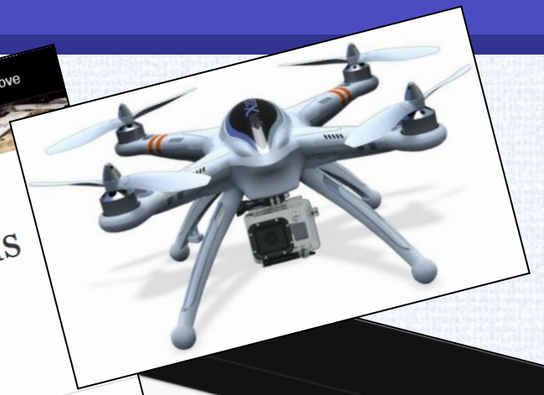












Sections The Washington Post Share Hazard Above

Play Video

PART THREE: NEAR MISSES

Close encounters on rise as drones gain in ularity

Story by Craig Whitlock

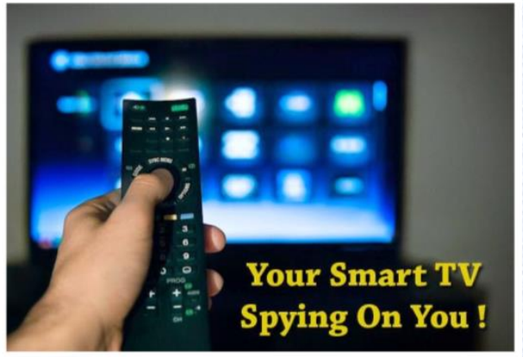
Published on June 23, 2014

The Hacker News™

Security in a serious way

Samsung Admits Its Smart TV Is Spying On You

Sunday, February 08, 2015 Mohit Kumar



ft creates bot you can chat with on Twitter

Search

SUBSCRIBE to get home del

2:34 p.m. EDT March 23, 2016

abc NEWS Election U.S. World Entertainment Tech

Microsoft's Chat Bot 'Tay' Gets a Time-Out After Rude Comments

By ALYSSA NEWCOMB

Mar 25, 2016, 11:03 AM ET

Share with Facebook Share with Twitter

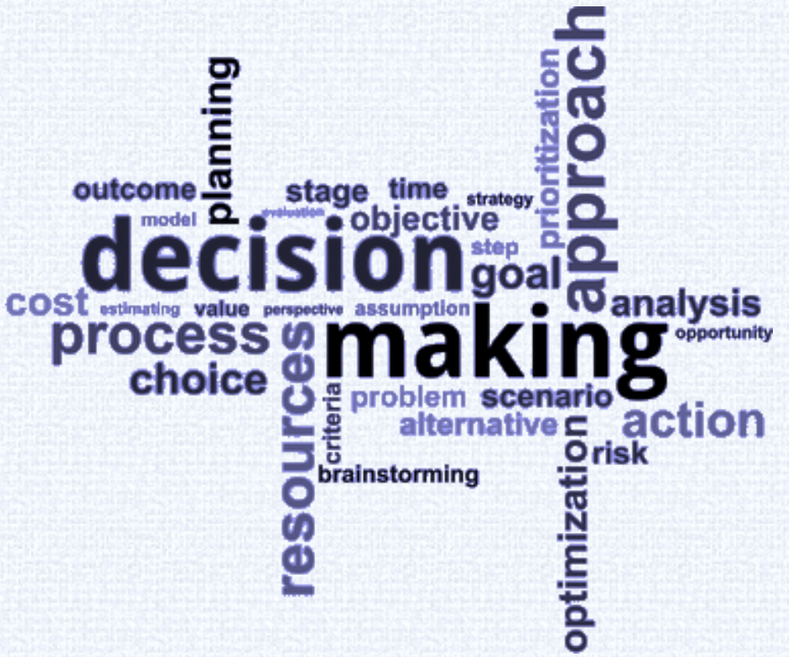
815 SHARES

Microsoft's teenage chat bot "Tay" is in a time-out of sorts after the artificially intelligent system, which learns from interactions on social media, began spewing racist comments within a day of its launch this week, company officials said.

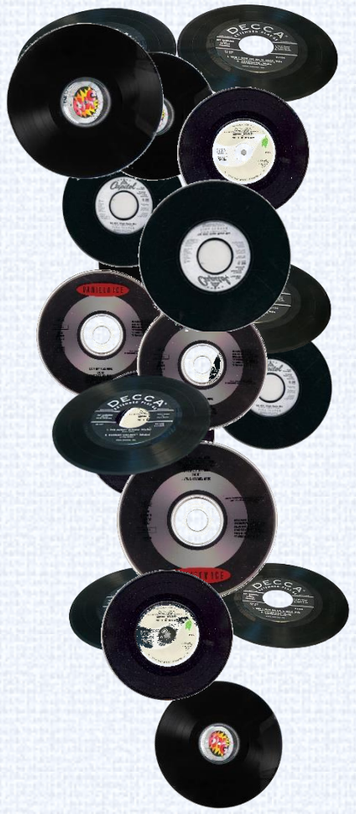
Geared toward 18- to 24-year-olds, Tay was launched as an experiment to conduct research on conversational understanding, with the chat bot getting smarter and offering a more personalized experience the more someone interacted with "her" on social media. Microsoft launched Tay on Twitter and messaging platforms GroupMe and Kik.

What to Secure and How Much is a Business Decision

- Cybersecurity is part of the risk picture.
- What functions are core to business?
- How much security can an organization afford to accomplish those functions?
- What else can create business-ending impacts?
- Fraud, security, and margins all matter.



What's Acceptable Loss? What's Acceptable Behavior?



Spearphishing
Drive-bys

Lateral Movement
Exposed Vulnerabilities

Media Leaks
Espionage

Insurance or Payment

Managed Response

Long-term Impact

Volume

Intent

HR Action

Long-term job impact

Criminal Prosecution

Balancing Priorities

Organizations

Adaptive ⟷ Standardized

Trust ⟷ Verify

Technology

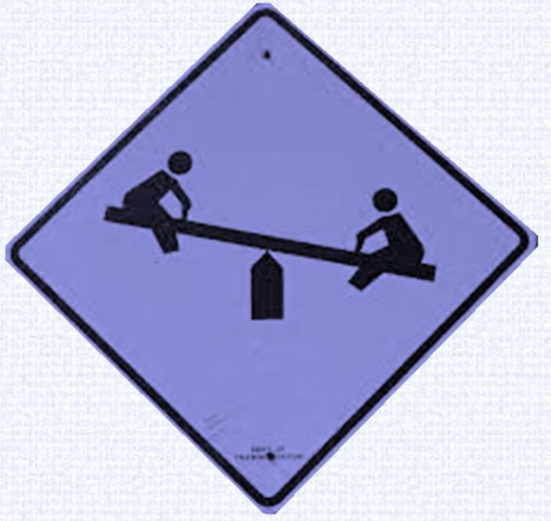
BYOD ⟷ Provided

DevOps ⟷ Legacy

Employees

Autonomy ⟷ Control

Privacy ⟷ Oversight

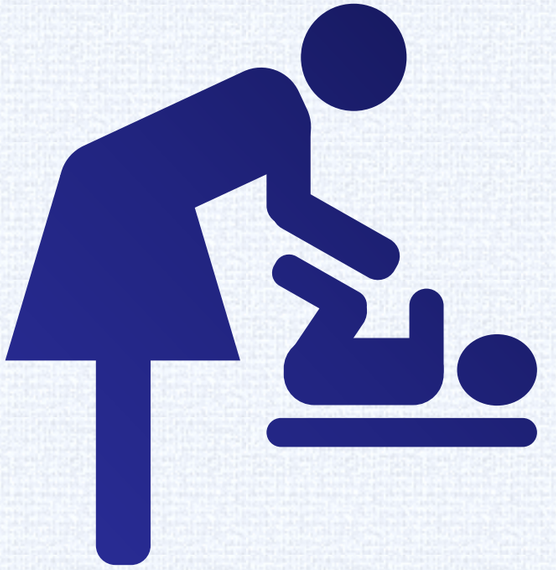


What about the Internet of Things?

Ch Ch Ch Ch Changes …

D. Bowie

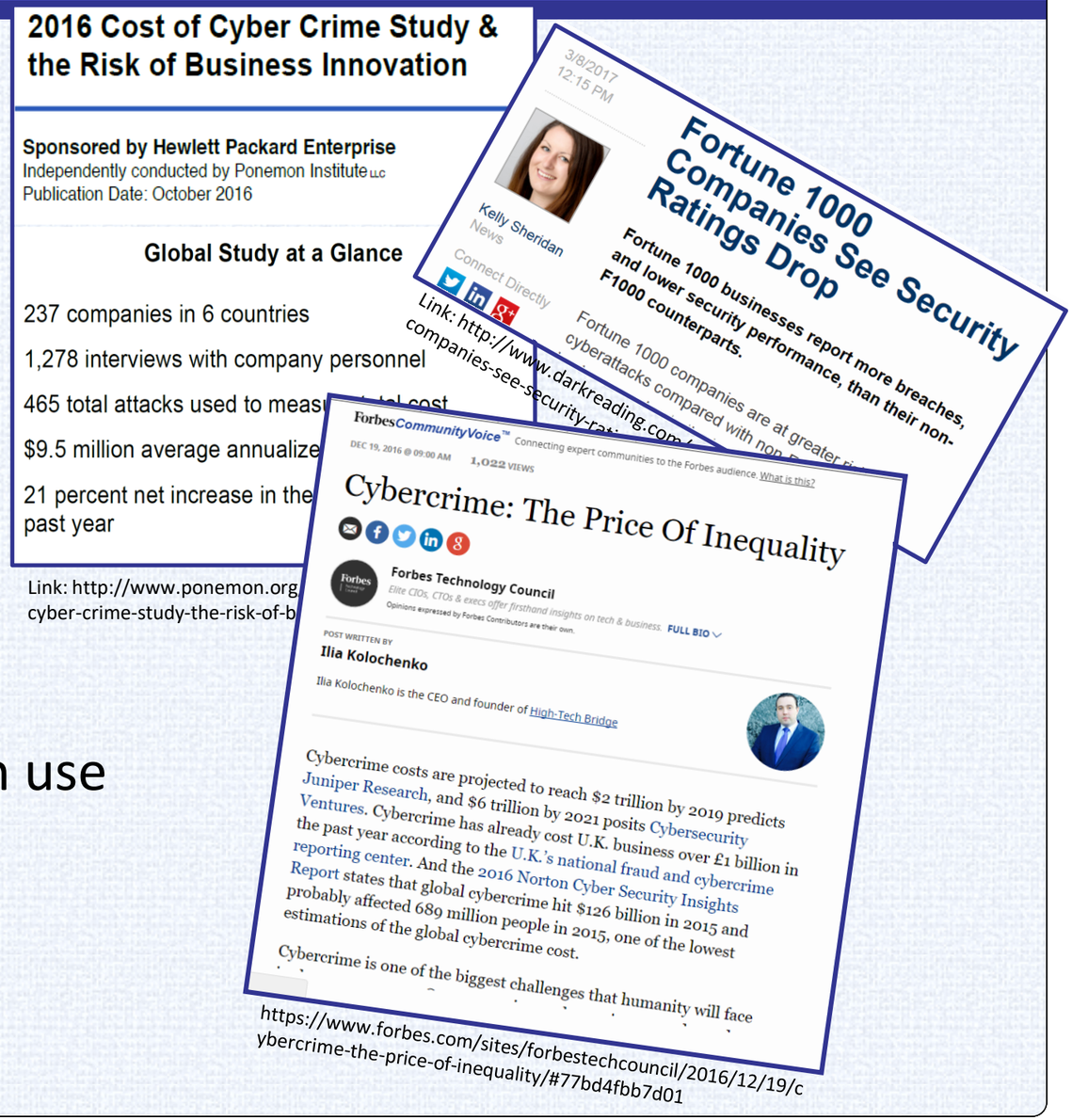
- **It's Hard to Keep a Security Perspective With …**
  - New lines businesses
  - Different competitive landscape
  - Mergers and acquisitions
  - Technology innovations
  - Reorganizations
  - People leaving, coming, being promoted, being demoted …



Changes leave people feeling vulnerable …
and that increases the insider threat.

The Costs and Opportunities Are Increasing

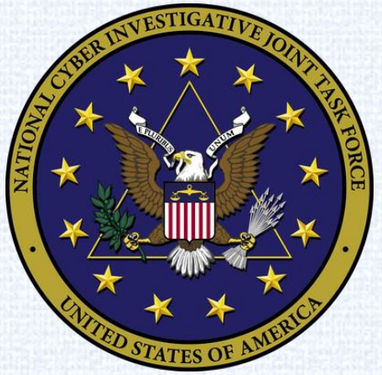
- Fraud enabled by IT
  - Traditional financial fraud by insiders and outsiders and combinations
  - Affects every type of organization
- Other Cybercrime
  - IP Theft
  - Sabotage
  - Approach is specifically logical, although it can use logical to attack physical
- As Businesses Move Online, the Threat Moves Online

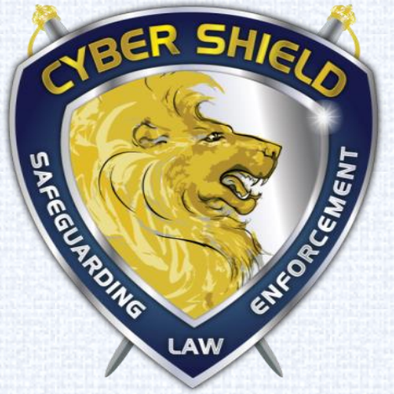


FBI Fights Cybercrime Across the Board

The FBI engages State and Local Law Enforcement officials in the fight against cyber crime through a number of different initiatives including:

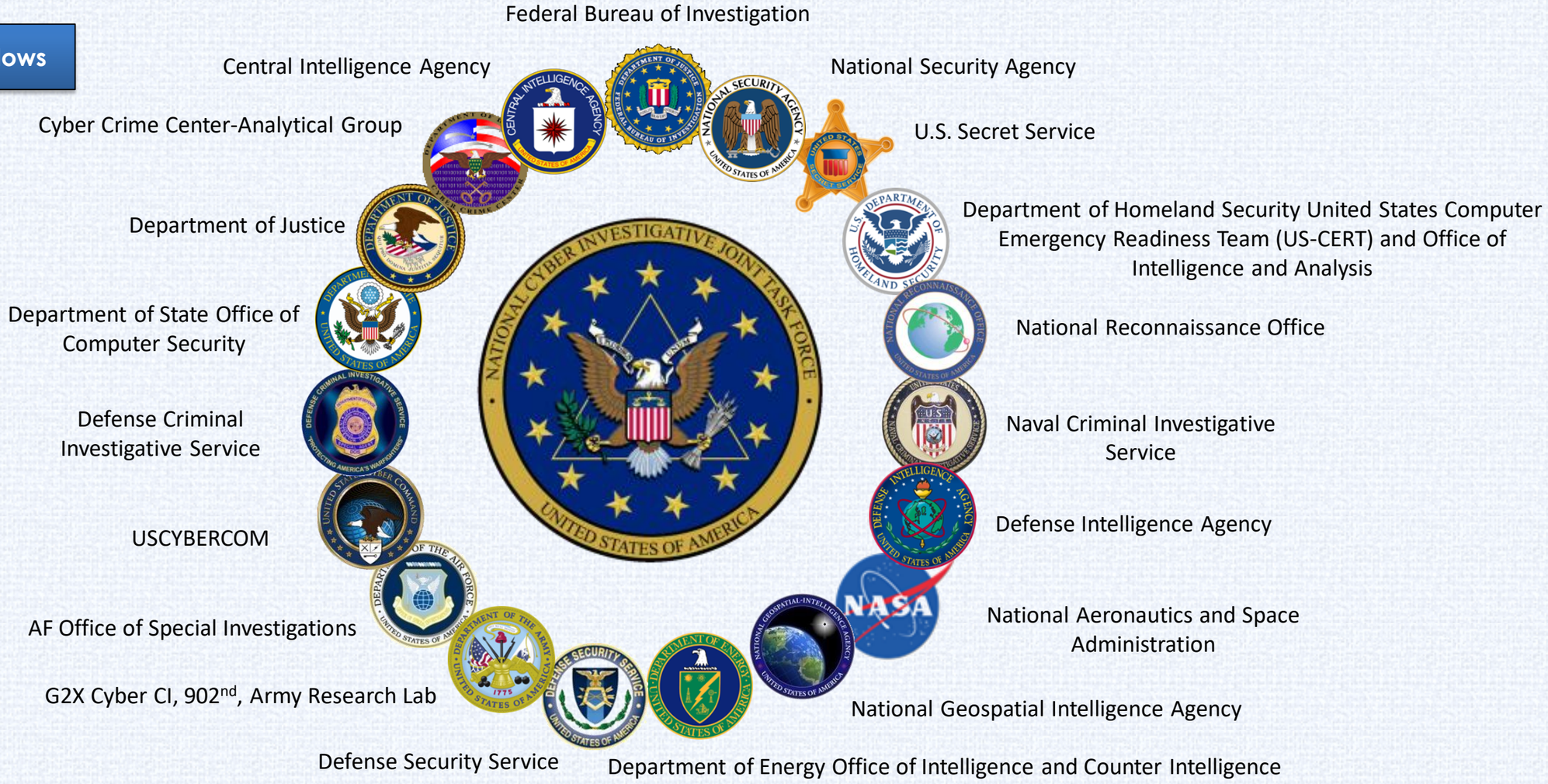
- National Cyber Investigative Joint Task Force
- Cyber Shield Alliance
- National Cyber-Forensics and Training Alliance





National Cyber Intelligence Joint Task Force (NCIJTF)

LE Fellows



InfraGard

- Information sharing partnership between FBI and public/private sectors to protect the nation's critical infrastructures.
- Over 25,000 members and more than 80 InfraGard Chapters through the United States.
- Access through the Law Enforcement Enterprise Portal (LEEP).

Access to Suite of Intelligence Products

Networking Opportunities

Alerts to Threats and Vulnerabilities

Understand Emerging Trends

www.infragard.org

Internet Crime Complaint Center (IC3)

- Intelligence Center for Internet Enabled Crime
- IC3 was established in May 2000
- More than 269,000 complaints received in FY2014 for a reported loss of more than $800M

Extortion

Romance Scams

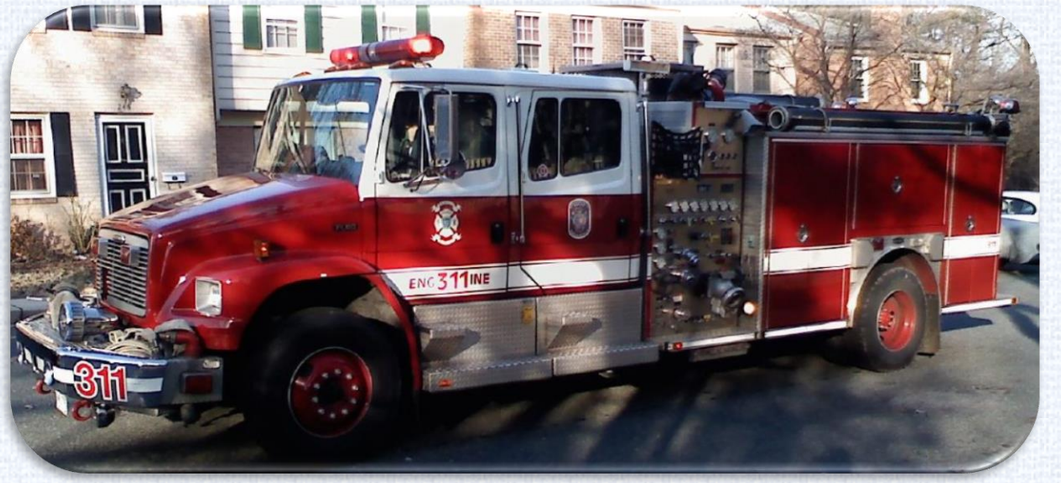
Mass Marketing Fraud

Auto Fraud

www.ic3.gov

Incidents Will Happen … Prepare and Practice!

- Internal and external, small and big
- Make the small ones routine and get used to the rhythm
- Prepare for the big ones before they happen



- Practice your Incident Response Plan, including:
  - **Senior Executives** – Who needs to know what, and when?
  - **General Council** – What can you disclose to who?
  - **Communication** – What are you telling your executives, your staff, the press, the public?
  - Conquer the stove-pipes

Report suspected cyber crime – Get to know your local FBI agent

Useful Links

- **Federal Bureau of Investigation**
  - https://www.fbi.gov/investigate/cyber
  - https://www.infragard.org/Application/Account/Login
- **National Counterintelligence and Security Center Resources**
  - https://www.ncsc.gov/index.html
  - https://www.ncsc.gov/issues/docs/Insider_Threat_Brochure.pdf
- **Carnegie Mellon's Software Engineering Institute**
  - http://www.cert.org/index.cfm
  - http://www.cert.org/insider-threat/cert-insider-threat-center.cfm
- Other
  - https://www.nacdonline.org/cyber