Thoughts On Current Information Technology Trends and Their Impact on Cybersecurity Implementation

Presented to the Maryland Commission on Cybersecurity Innovation and Excellence

August 27, 2014

Daniel Mintz

What We Will Talk About Today

- Introduction
- IT Technology Thoughts
- Cybersecurity Implications
- Policy Thoughts

Introduction - Personal

- Local
  - Born in Southeast Washington
  - Grew up in Silver Spring
  - Went to all local public schools
    - Four Corners Elementary
    - Sligo Jr High (now Sligo Middle)
    - Northwood (was Indians, now Gladiators)
  - Graduated from the Unversity of Maryland College Park with a BS in Information Systems Management
    - Worked my way through school at the Computing Center
  - Masters in Information Management from UMUC
  - Live in N. Bethesda (Windermere)

Introduction - Professional

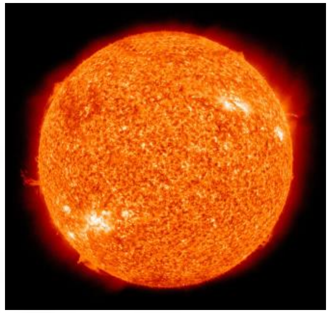
- Learned to program in High School as an Explorer Scout sponsored by Vitro Corporation, then in Aspen Hill (mid-1960's)
- Worked for integrators around the Beltway for many years as a programmer, systems analyst, and program manager; before joining the government worked 11 years at Sun Microsystems
- Served as the Chief Information Officer at the US Department of Transportation from 2006-9
- After Government service, CTO and then a COO, the latter to a small woman-owned company in Gaithersburg
- Adjunct Professor at UMUC
- Senior Advisor to a non-profit created to increase the involvement of the academic community with Government, the Advanced Technology Academic Research Center (ATARC)
- Run a <very> small consulting company ESEM Consulting LLC

IT Technology Thoughts

- Cha-cha-cha-changes in
  - Systems architecture
  - Networking and the Internet of Things
  - Users becoming more participatory
- Transactional economics and its long-term implications

Changes in Systems Architecture

Earth Centered – Ptolemaic
The target is the user (functional)



Sun Centered – Copernican
The target is the data (object oriented)

Nothing Centered – Warhol
We do not know what the target is

Our focus historically has been on efficiency.

Now the focus shifts to agility and rapid change.

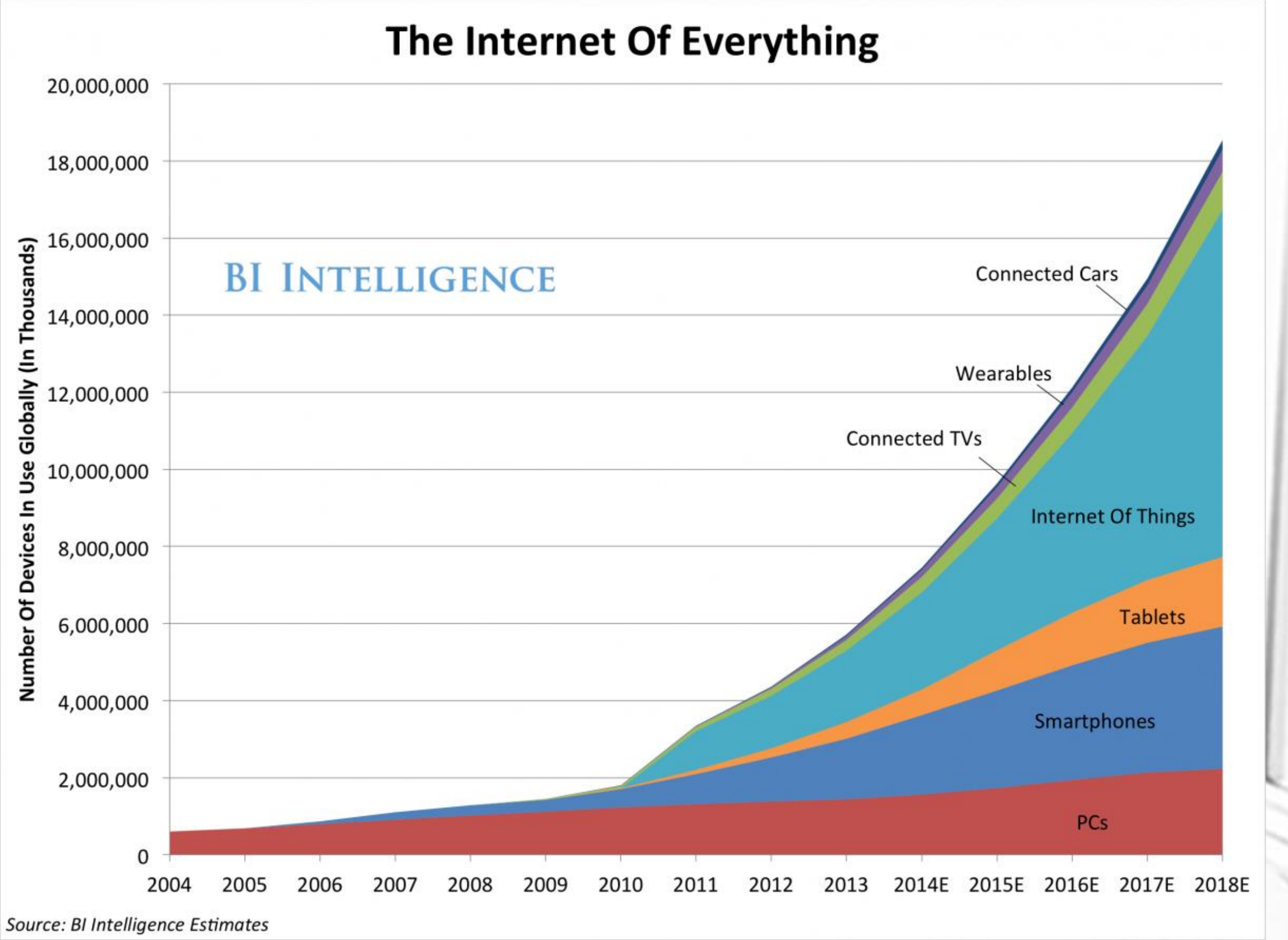
Most organizations, especially governmental organizations, are much better at efficiency (at least as a goal) not agility. This is a big change, not entirely recognized.

Changes in Networking and the Internet of Things (IoT)

- Google will be 16 years old next week
  - In 2013, average of 5.9 billion searches/day
- Facebook was 10 years old in February, 2014
  - One billion active users September, 2012
- YouTube was 9 years old in February, 2014
  - One billion users/month, six billion hours are watched each month, 100 hours of video are uploaded every minute
  - More people aged 18-34 in the US watch YouTube than any cable network
- Twitter was 8 years old in March, 2014
  - In 2013, average of 340 million tweets/day
- Current generation shares information on-line, not so great for cybersecurity

Internet of Things (IoT)

- 2013: close to 10 billion connected devices
- 2020: 30-50 (or more) billion connected devices
- Over 1 trillion sensors by 2017 (per HP Labs)
- Wearables are becoming medical devices (big policy implications)
- Not so much thought to security issues



Source: BI Intelligence Estimates

Users becoming more participatory

- Co-creation (or co-production) results when an organization and its customers are both involved in creating the resulting product
- A commercial example is YouTube where the company basically provides the infrastructure to load, search for and view video's. Customers produce almost all of the actual content
- This has just started in the Government space
  - NOAA uses citizens to provide data for weather reports
  - NASA has solicited customer input to help analyze pictures
- We may find over time that the definition of Government services will change – it took 20 years before people realized that TV was not radio with pictures, it may take that long to understand that the Government + the Internet is different than just on-line Government services

3D Printing/Additive Manufacturing

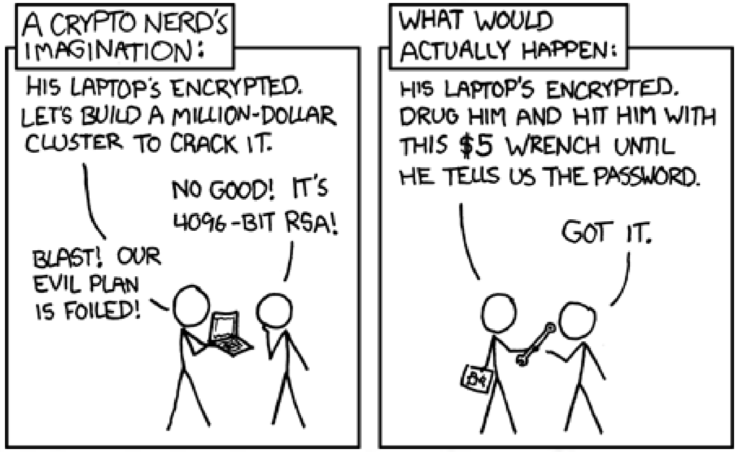
- Mary Huang started a company called Continuum in Brooklyn
  - She prints shoes using 3D printers
  - She is looking to email her designs to 3D printers overseas to be printed there
- An Italian shoe manufacturer sells 3D printed shoes for $99/pair or one can get the model for free and print it at home
- In healthcare, it will be possible to print livers, ears, hands and eyes. In the next few years, it will be possible to print skin for skin grafts
  - One of the big advantages is the ability to produce customized implants for surgery, currently useful for implants in particular hearing aids
- Beginnings of a revolution in manufacturing, how it is capitalized, regulated and taxed

IT Technology – Transactional Cost Economics

- In 1937 a British economist Ronald Coase wrote *Nature of the Firm*
  - To understand economic systems one needs to understand the costs of performing a transaction
  - He asked the question 'why should a company have an internal purchasing department'
- The Internet reduces transaction costs
  - Thus over time activities that typically were performed internally within organizations potentially could move outside

Cybersecurity

- My cousin the Dermatologist
- Risk management
- The problem of false positives
- Thoughts on what to do
  - Security hygiene
  - OODA Loops and Biological Designs


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Chinese Hackers Pursue Key Data on U.S. Workers – NY Times

DHS contractor suffers major computer breach, officials say – The Washington Post

U.S. Retailers Warned Of Possible Hacking – Huff Post

More than 1,000 U.S. retailers could be infected with malicious software lurking in their cash register computers …

Risk Management

- Risk Management requires prioritization, this is hard to accomplish
  - No one wants to take ownership of the un-prioritized risk
- If we try to protect everything everywhere we will end up protecting nothing anywhere, so risk management is necessary
- Requires consistent attention and a willingness to expose problems

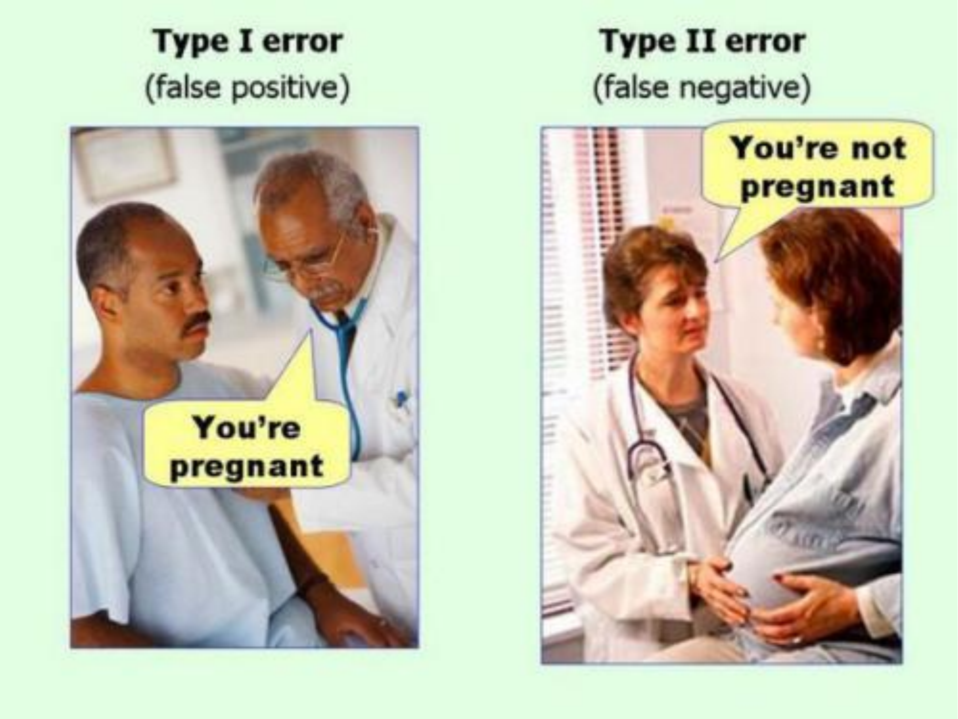
"We've considered every potential risk except the risks of avoiding all risks."

The problem of false positives

- The biggest problem with security (and other types) of oversight activities are false positives

- The average time required to detect a breach is 229 days – Mandiant 2014 Threat Report
  - Top challenge was too much data, too many alerts and too many false positives

- The goal is to maximize the identification of false positives in some automated fashion

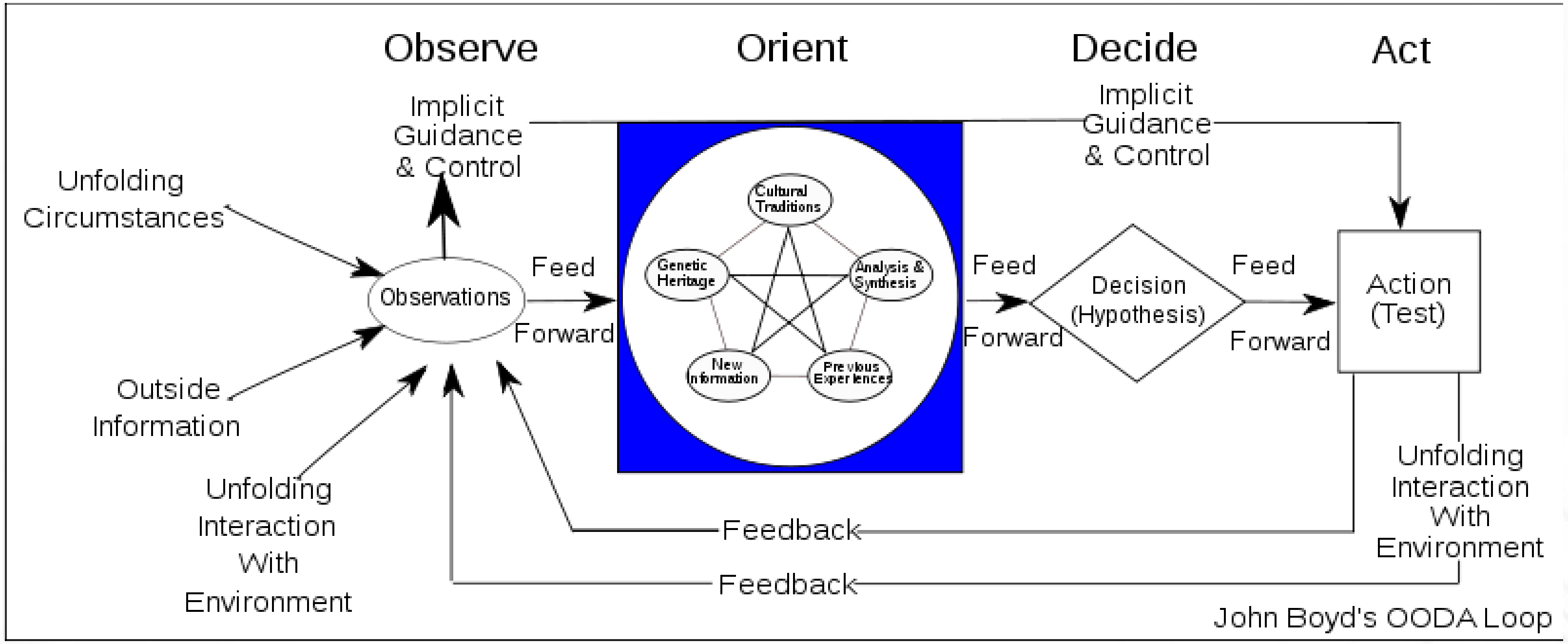


Security Hygiene

- Build security into the budget process
- Prioritize security controls, deal with the most important first
- Keep software current, formal ‘patch’ policies
- Accurate situational awareness
- Tracking data in and out
- Aggressive oversight (comparable to the Federal Inspectors General)
- Status transparency

OODA Loops

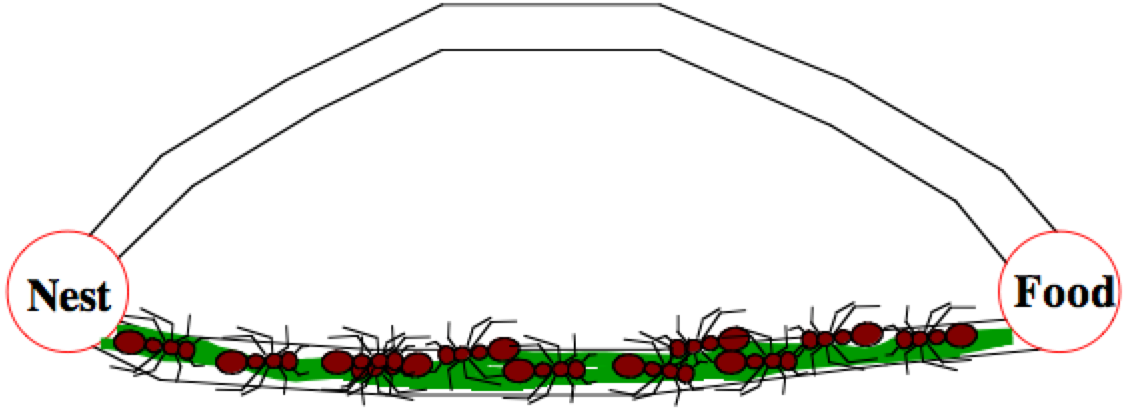
- Developed by USAF Colonel John Boyd
  - “In order to win, we should operate at a faster tempo or rhythm than our adversaries”



John Boyd's OODA Loop

Biological Designs

- Stigmergic systems: a mechanism of indirect coordination between agents or actions
- Self-organizing
- Adaptable to unpredictable situations
- Reactively resilient
- Proactively innovative
- Systems-of-systems



Policy Thoughts

- Regulatory barriers
  - Get rid of them
- Government Fellows
  - GSA has a good model
- It’s the data, stupid
  - Decide what to protect
  - Data standardization
- Transparency (already good steps in place)
- Agility probably means moving as much as possible to the cloud
- Co-creation can tie to citizen outreach in general

© Cartoonbank.com

“Hannibal got elephants over the Alps. Bearing that in mind, somebody think of something.”

Thank-You

Daniel Mintz

dmintz@esemconsulting.com
dmintz@atarc.org
dmintz@umuc.edu

301-332-0717/c
@technogeezer
Blog: http://www.ourownlittlecorner.com