

SAINT PAUL COLLEGE ACM CLUB CYBER SECURITY WORKSHOP

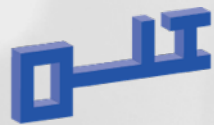
Wednesday, 09 April 2014 0800.1500 CT
First Floor Auditorium



Matthew J. Harmon



President
(ISC)2 Twin Cities MN
isc2tc.org



IT RISK
LIMITED

Owner & Security Researcher
IT Risk Limited
itriskltd.com



SANS Instructor and Mentor for Cyber Aces



Organizer
Security B-Sides MSP 2014
BSidesMSP.org



United States National Body
Liaison Officer & Subject Matter Expert

CISSP, GSEC, GCIH, GCIA
matthewjharmon.com

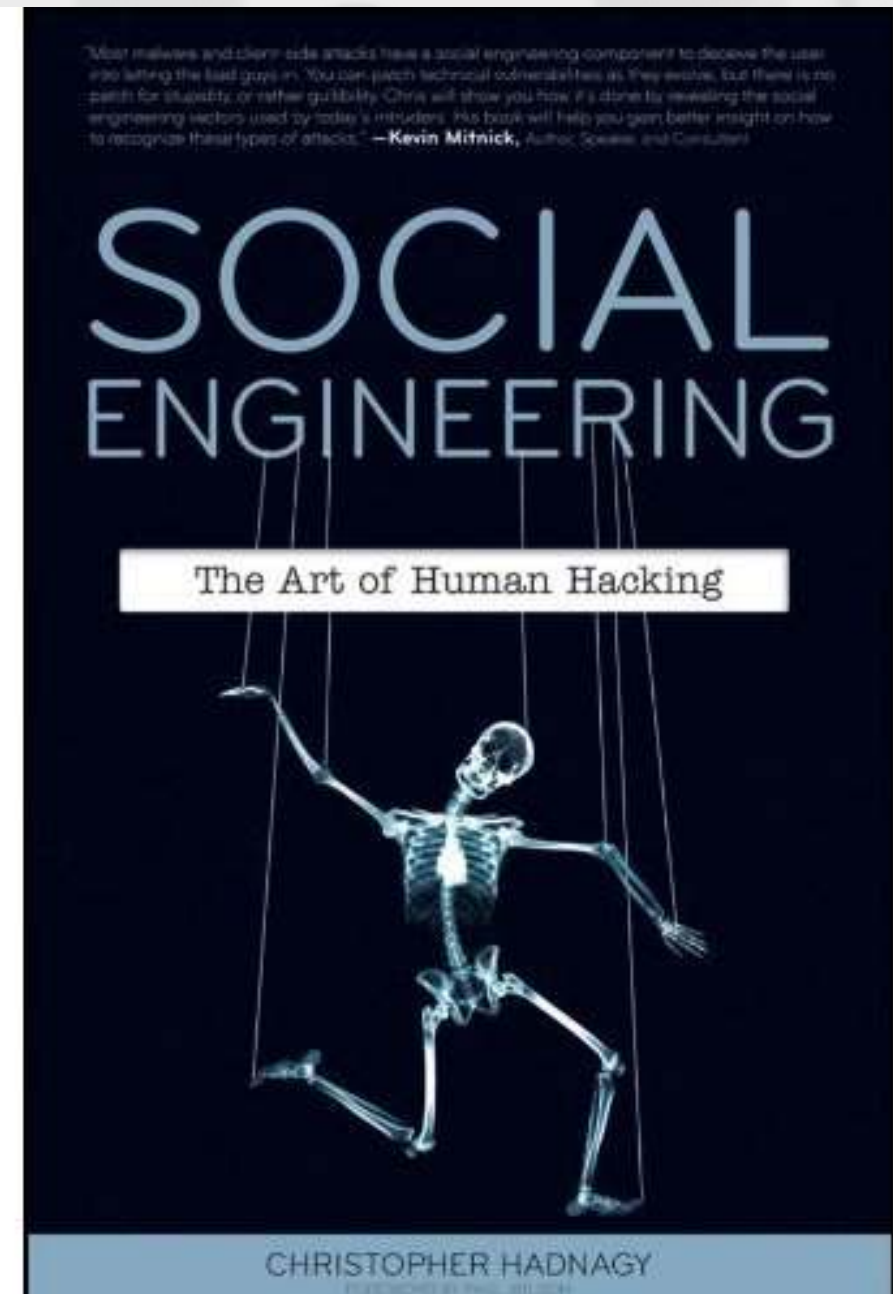
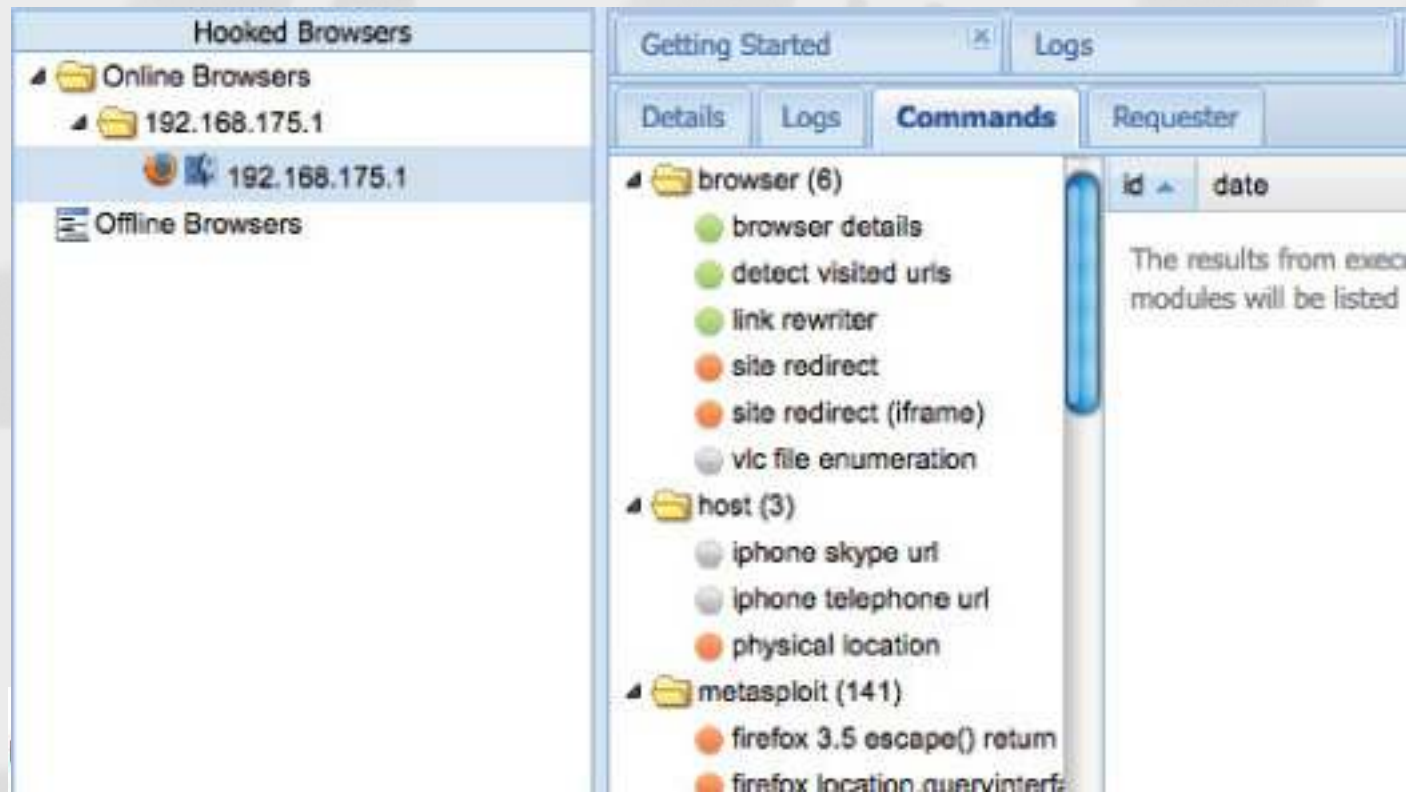
Cyber War
is it this?



**PROACTIVE CYBERSECURITY
IS CONTROL OF YOUR NETWORK
BEFORE AN ATTACK HAPPENS.**

 **Symantec.**

Maybe this?



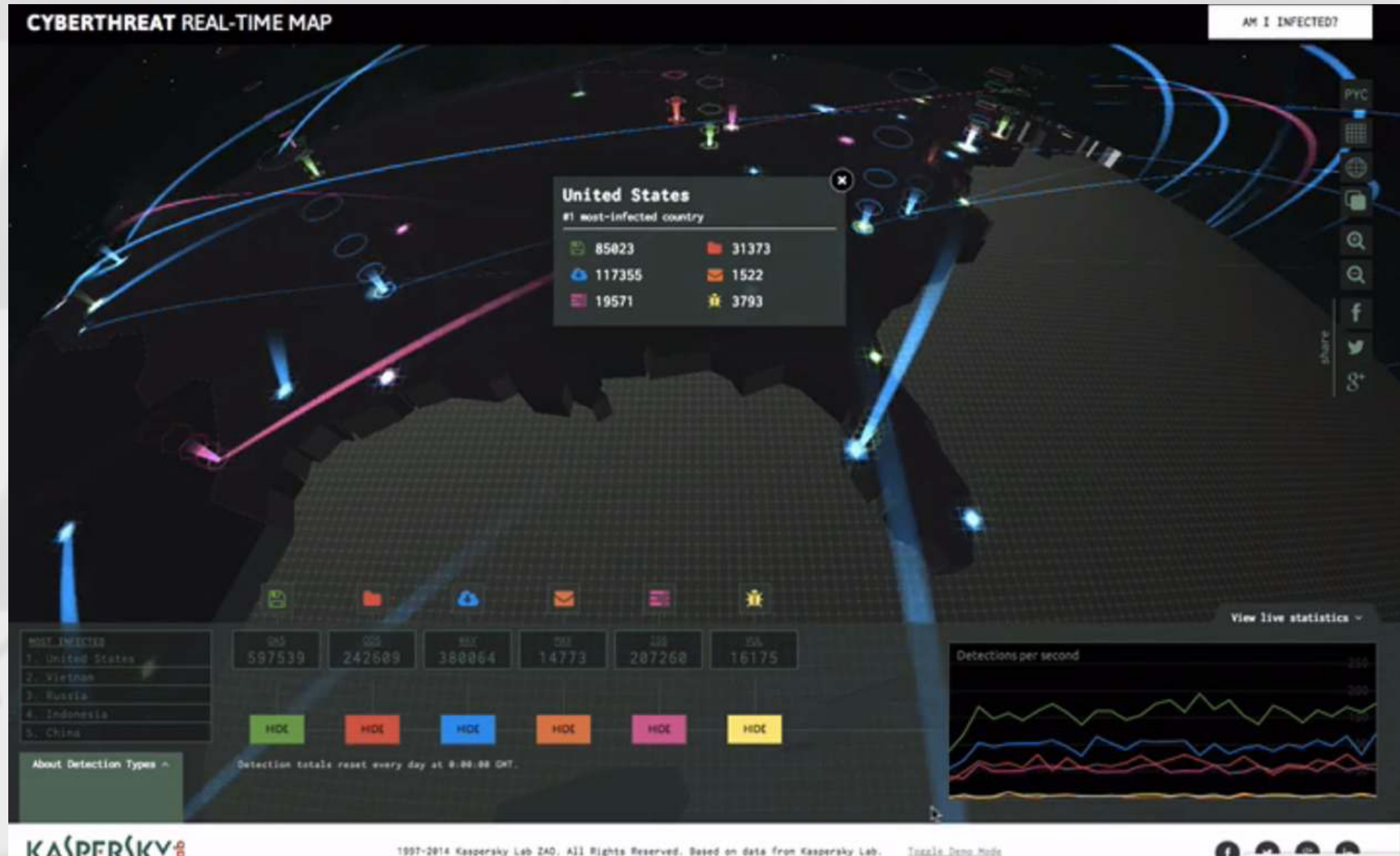
“It is much easier to trick someone into revealing a password for a system than to exert the effort of hacking into the system”. Kevin Mitnick

Or this?



Attack Map Video [2] Source:
map.ipviking.com

Or this?



Attack Map Video [2] Source:
cybermap.kaspersky.com

Actually, it is more like this



and this...



Our adversaries are massively overcapitalized and have many more resources than we do.

They don't fight for a "security budget".
They have research and development budgets.
They have all the time in the world.

They only have to find one
exploitable vulnerability to pivot from

State of the Union



The largest breaches... so far.

Adobe (2013): 152 Million Records

Heartland (2008): 130 Million Payment Records

Target (2013): 110 Million Records

T J Maxx (2007): 94 Million Transactions

TRW (1984): 90 Million Credit Reports

Sony (2011): 77 Million Records

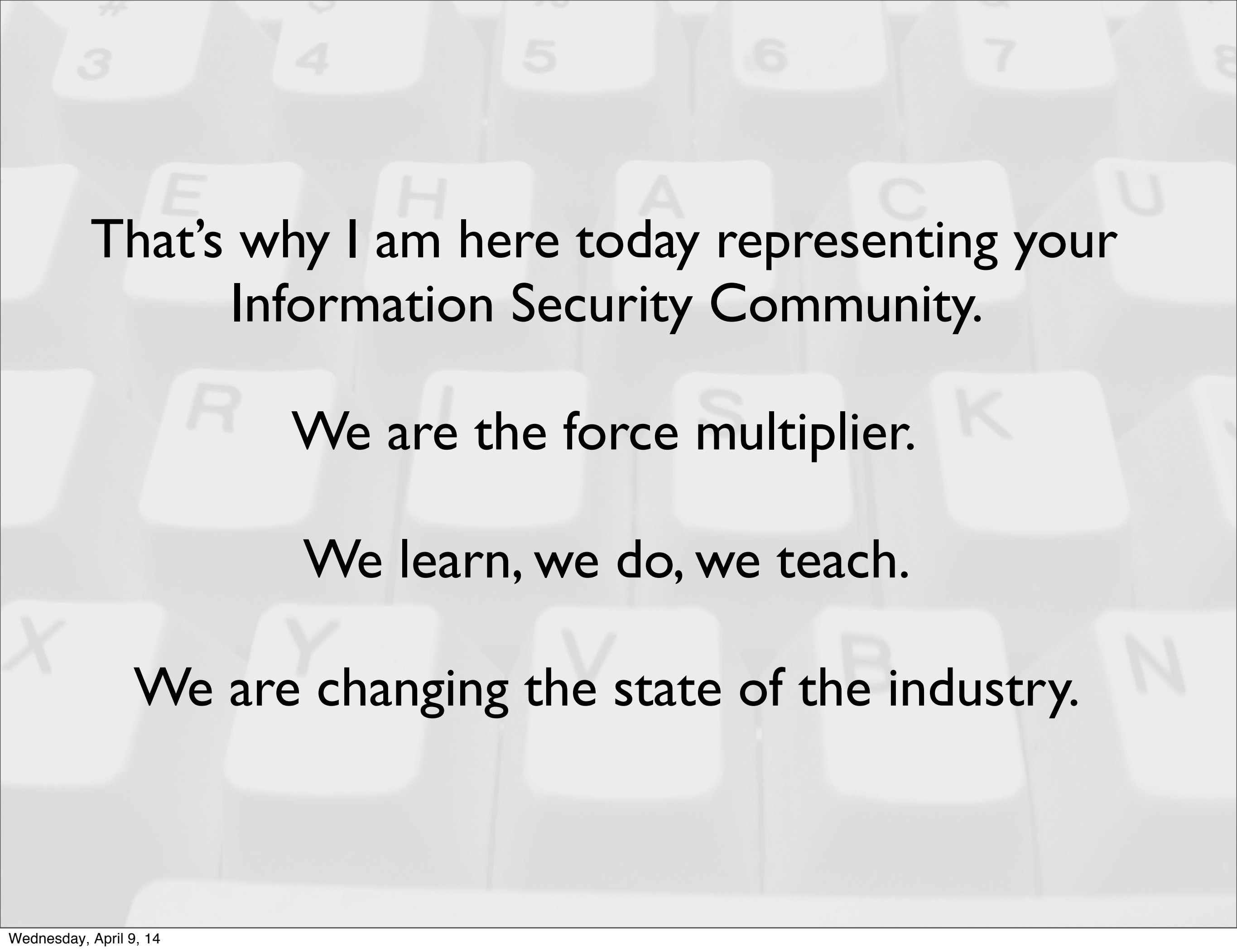
Card Systems Inc (2005): 40 Million

Rock You Media (2009): 32 Million

US Dept of Veteran Affairs: 26 Million



They all had anti-virus, firewalls, intrusion detection systems, certifications, multi-million dollar security programs, security staff but were still compromised.



That's why I am here today representing your
Information Security Community.

We are the force multiplier.

We learn, we do, we teach.

We are changing the state of the industry.

We have the Defenders Advantage

**We (should) know our networks and systems
better than our adversaries.**

**We setup traps. We setup fake devices.
We go on the offensive.**

Active Defense Harbinger Distribution (ADHD)
<http://sourceforge.net/projects/adhd/>

Computer Security Careers used to be...

- Mac User Groups, Linux User Groups, Windows User Groups
- Usenet, Internet Relay Chat, Mailing Lists
- Start out as a
 - Systems Administrator or Network Administrator
 - then specialize in “security”, which was configuration management, incident response, policy or IT Audit
- ISACA - CISA, (ISC)2 - CISSP, 2600 Magazine Meet-ups

Now we have Cyber Security Careers

- Degree tracks like those here at St Paul College
- ACM taking on Cyber Security Workshop
- SANS Institute Certification programs
- International standards - SC 27 “IT Security Techniques”
- NIST Cyber Security Framework and NIST SP800 Series
- Very **flexible** industry with NEGATIVE 4% Unemployment
- Cross training and cross over in job roles
- Greater Twin Cities Metro is an **Innovation Sector**

Where do I want us tomorrow?

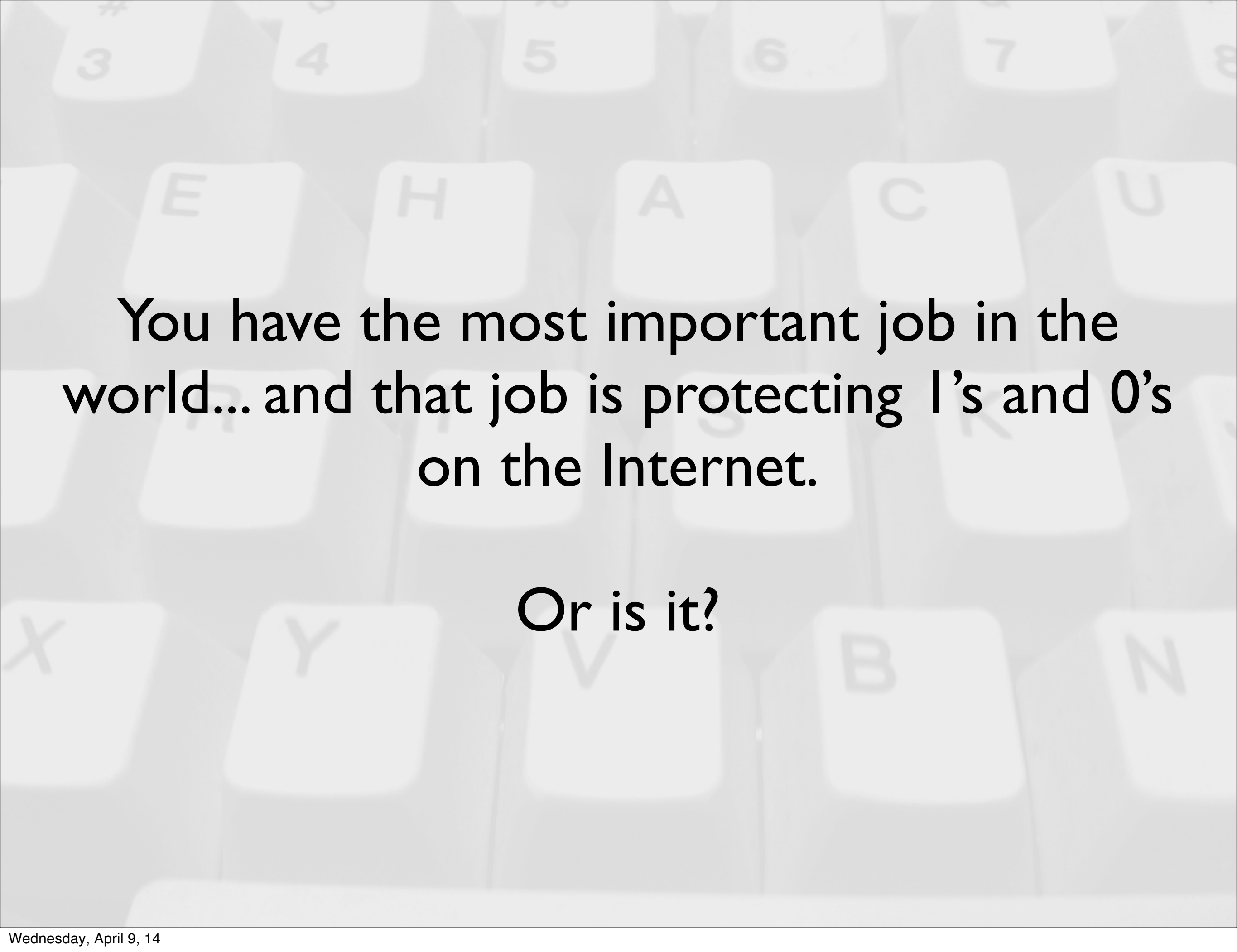
Resilient Computing & Businesses

- Degree Tracks + **Apprenticeships** for New Professionals
 - Must be nimble: Constantly changing industry and environment
- **Cyber Security Center of Excellence** for Businesses
 - Locally applicable technical controls
- Scripted Systems Administration (Humans Hands-Off)
 - Ansible, Puppet, Chef
- Private Security Intelligence Officers?
- Silicon Plains? Silicon Lakes?

Many Groups and Specialties

- MN-ISSA, (ISC)2 Twin Cities, DC612
- ISACA, BCPA, Cloud Security Alliance
- HTCIA, HI TECH

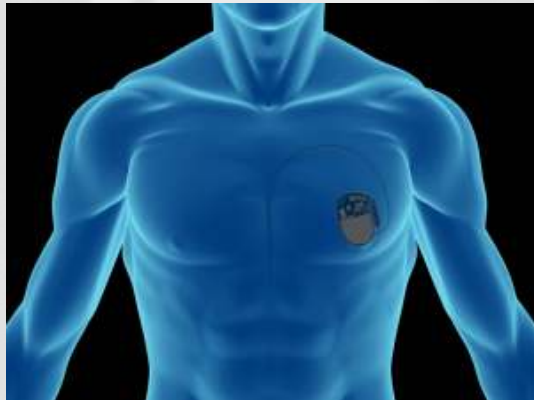
- We must work together
- Cooperation instead of Competition



**You have the most important job in the
world... and that job is protecting 1's and 0's
on the Internet.**

Or is it?

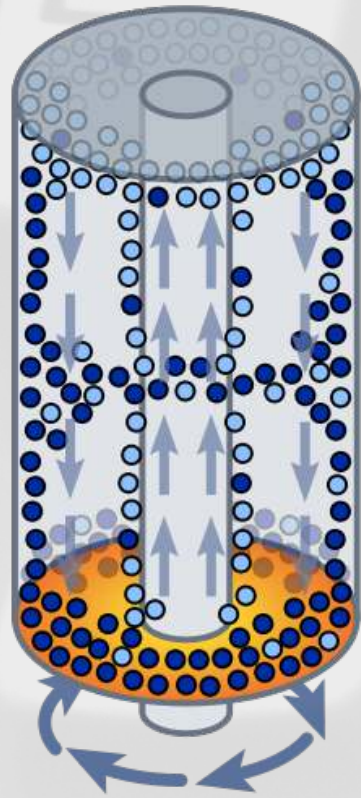
What about the Internet of Things?



Heart Pace
Makers
Blood Insulin
Pumps

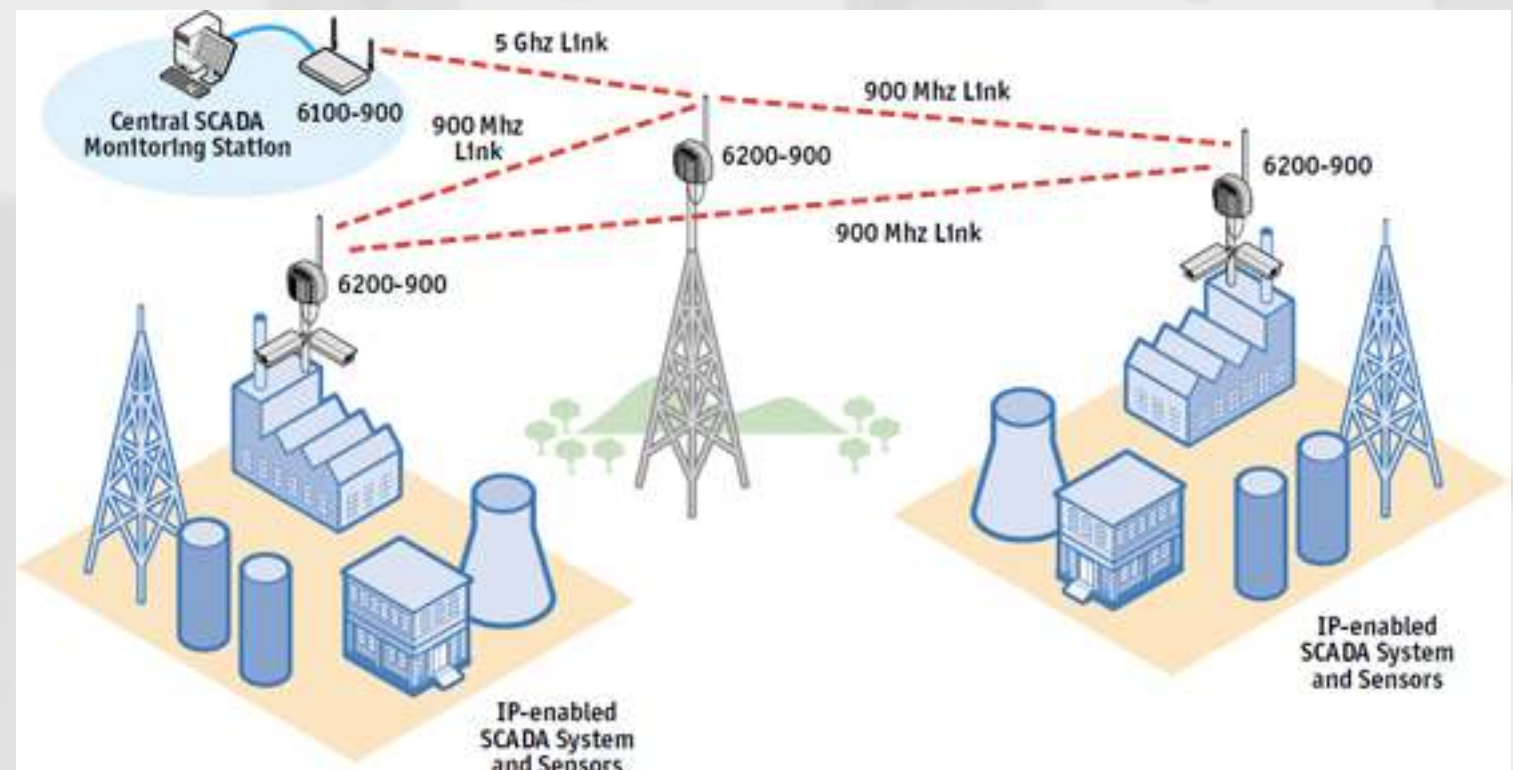
Bluesnarfing
Bluejack
Bluebug

or our Critical Infrastructure?



Zippe-type gas centrifuge with U238
and U-235 (TCP/IP over Serial)
Attacked by Stuxnet

900 Mhz backhaul
Weak encryption



Hacked out of Business



Matthew J. Harmon



matthewjharmon.com

Check out :

SecurityWeekly.com

isc2tc.org

DarkReading.com

isc.sans.org

DataLossDB.org

cybermap.kaspersky.com

map.ipviking.com

sans.org/critical-security-controls

This work is licensed under the Creative Commons Attribution-NonCommercial 3.0 Unported License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-nc/3.0/> or send a letter to Creative Commons, 444 Castro Street, Suite 900, Mountain View, California, 94041, USA. This presentation may contain images owned by others, where possible citation has been provided and all rights are held by their respective parties unless otherwise noted.

© Copyright 2014 Matthew J. Harmon All rights reserved.

