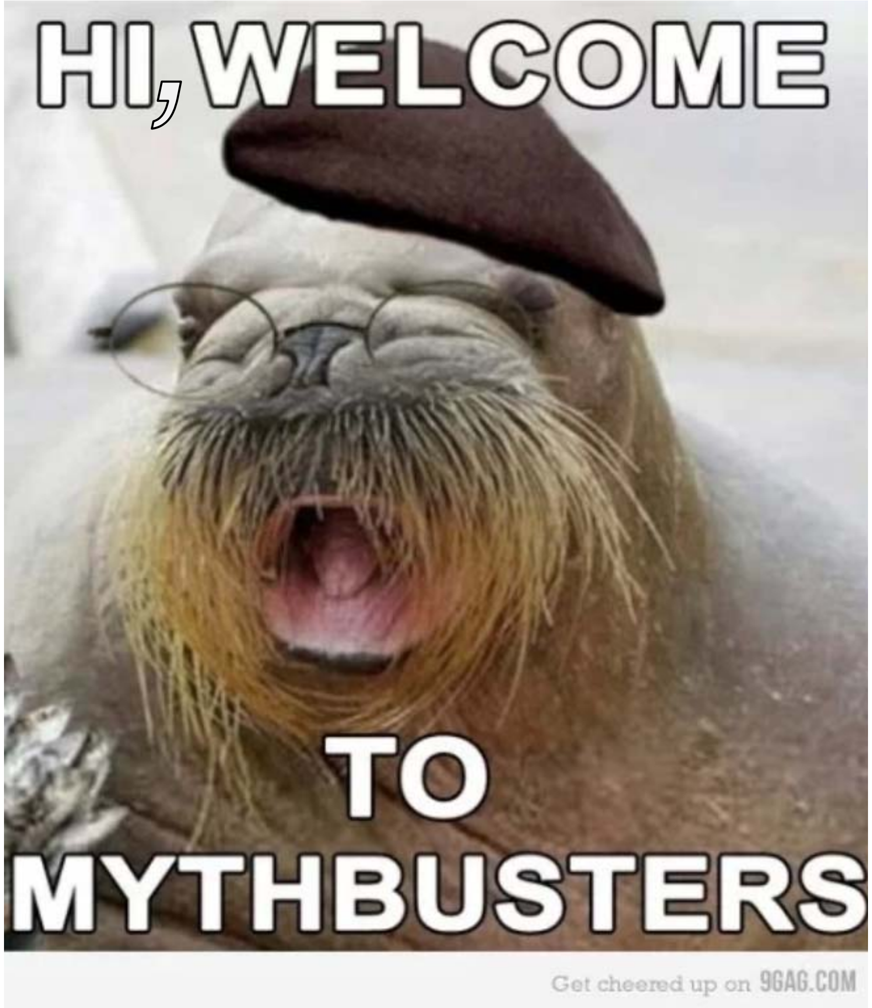
Cybersecurity OT&E Myths

14 April 2015

Walter Dodson, Kevin Eveker, Anil Joglekar, Sourav Mandal,

William Robbins, Phillip Webb, and Kevin Westburg

Shawn Whetstone, Project Leader


HI, WELCOME
TO
MYTHBUSTERS
Get cheered up on 9GAG.COM

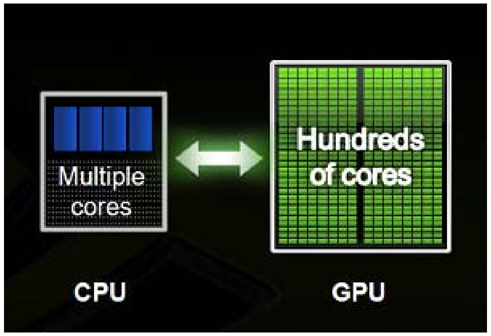
Myth 1: Breaches are preventable

- **Long, complex passwords aren't enough.**
  - E.g., CyberVor (2014) or GPUs

- **Does it use electronics? It can probably be compromised.**
  - E.g., tanks, helicopters, radar, and rocket launchers

- **Classified networks can be compromised.**
  - E.g., SIPR and other networks

- **Air-gapped systems can be compromised.**
  - E.g., TEMPEST program



Credit: InfoSec Institute

- **No matter the system, always assume it has been breached**

Known active insiders on classified networks

Average Time Active in Months: 53

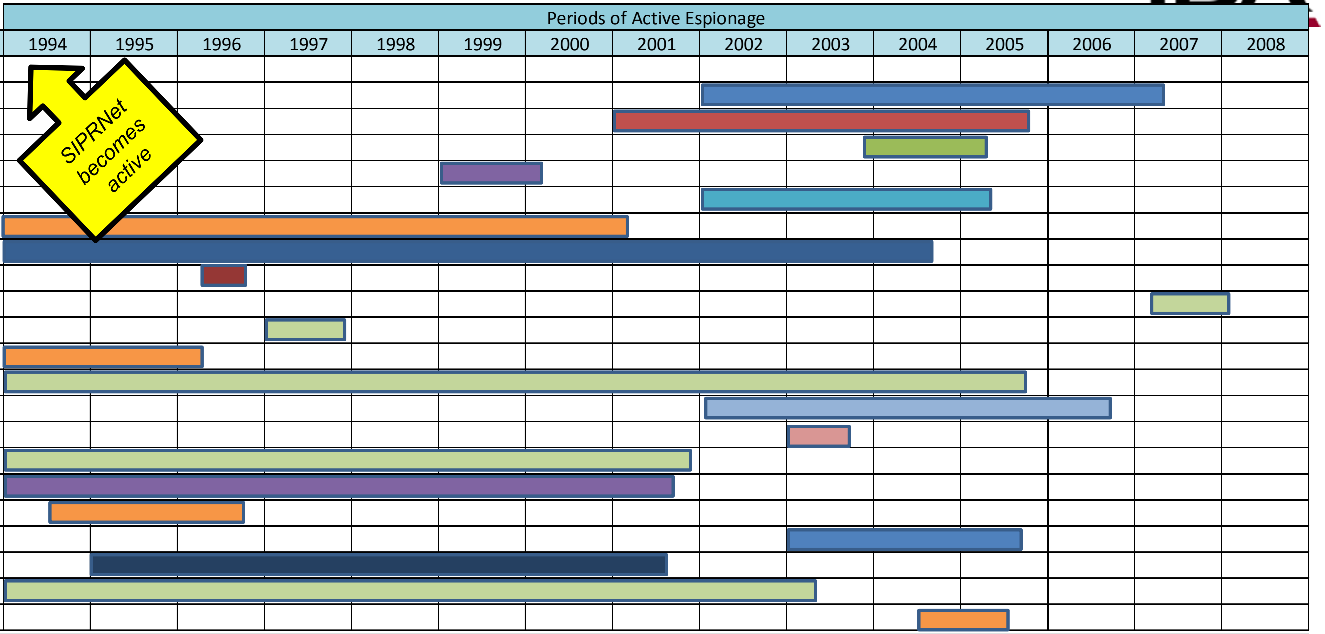
Only 3 of 21 had significant computer skills

They all worked alone.

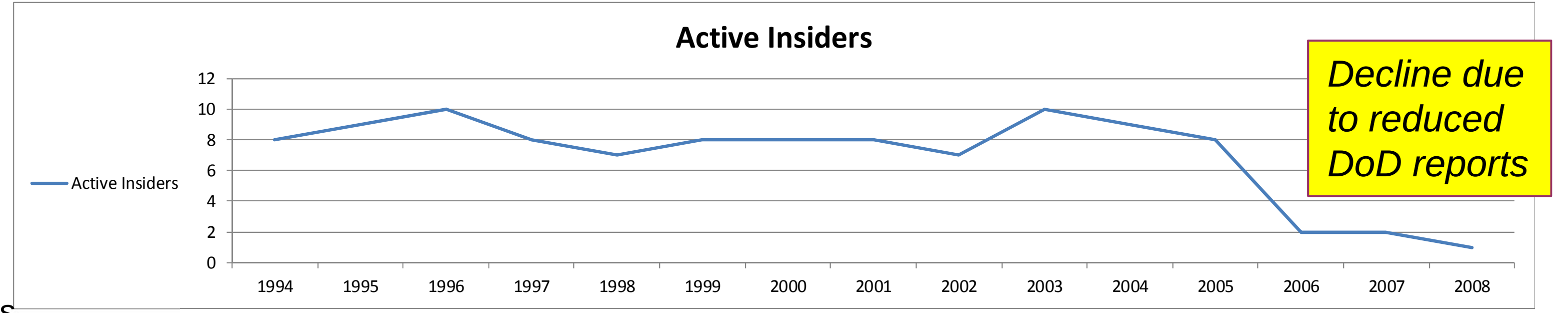
20 of 21 were men

18 of 21 were volunteers

Last Name	Start Date	End Date
Abu-Jihaad	1/1/2002	3/27/2007
Aragoncillo	1/1/2000	9/10/2005
Diaz	12/1/2003	3/1/2005
Faget	1/1/1999	2/17/2000
Franklin	1/1/2002	5/3/2005
Hanssen	3/3/1994	2/18/2001
Keyser	3/3/1994	9/15/2004
Kim	4/1/1996	9/24/1996
Bergersen	3/1/2007	2/11/2008
Lee	1/1/1997	12/8/1997
Lessenthien	3/3/1994	4/22/1996
Mak	3/3/1994	10/28/2005
Maziarz	1/1/2002	10/1/2006
Mehalba	1/1/2003	9/23/2003
Montaperto	3/3/1994	12/1/2001
Montes	3/3/1994	9/21/2001
Nicholson	6/27/1994	11/16/1996
Nour	1/1/2003	9/1/2005
Regan	1/1/1995	8/3/2001
Smith	3/3/1994	4/9/2003
Weinmann	10/1/2004	7/1/2005

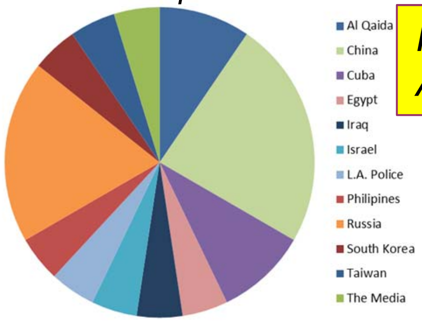


SIPRNet becomes active



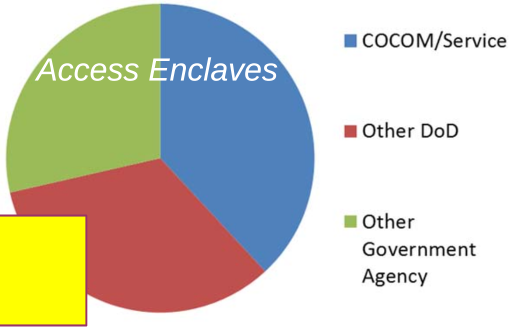
Decline due to reduced DoD reports

Data Recipients

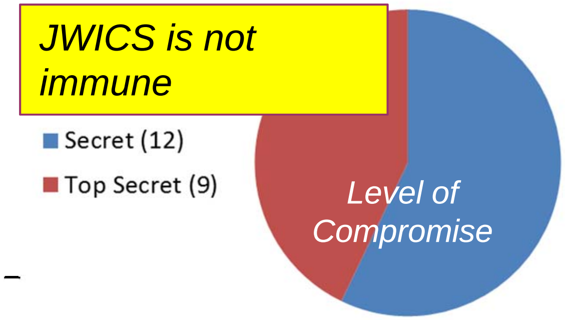


Friends and Adversaries

It's not just COCOMS



JWICS is not immune



Myth 2: Cybersecurity is not my responsibility

- **Anti-virus only works on known malware.**
  - Does not entail all vulnerabilities (e.g., incorrect firewall rules)
- **Intrusion Detection Systems (IDSs) need data.**
  - Attackers can obscure logs.

OSSEC

Open Source IDS

- **IT professionals are imperfect.**
  - Cyber defenders miss alerts or are slow to react
- **Mantra: protect, detect, react, and restore (PDRR)**
  - Defense-in-depth, a practical strategy for IA

Myth 3: Cybersecurity is a product

- **Good cybersecurity is a process.**
  - – A stationary warrior is unlikely to defeat a dynamic adversary

Credit: *Wikimedia Commons*

Sun Tzu

- **Regularly update.**
  - – Protect
  - – Software, firmware, anti-virus, and HIDS

- **Regularly review the systems & devices.**
  - – Protect
  - – Accounts, privileges, passwords, services, network

- **Regularly check the defense-in-depth.**
  - – Detect, react, restore
  - – Tactics, techniques, and procedures (TTPs)

Myth 4: Cybersecurity testing is optional

- **If it uses electronics, it is theoretically susceptible.**
  - E.g., tanks, helicopters, radar, and rocket launchers
- **Authority to Operate (ATO) is only a first step.**
  - “Will this system present an unacceptable risk to the rest of the network?”
- **Controls compliance is an additional consideration.**
  - “How should we operate the system?”
- **Assuming breach, testing measures the impact.**
  - Defense-in-depth mantra: protect, detect, react, and restore

Myth 5: This system isn’t worth the effort

- **Tell that to Sony.**
  - E.g., Female star paid ~2% less than male leads = lawsuits
- **Every system contains potentially usable information.**
  - E.g., information about other systems or classified information
- **Unfortunately, usernames and passwords are often recycled.**
  - E.g., Dropbox (2014)

Myth 6: Intrusion detection is sufficient

- **Without a plan, the only recourse is to shut down.**
  - Mission compromised
- **You may not have identified the attacker.**
  - Future missions at risk
- **You may not know what information has been lost.**
  - Current & future missions at risk

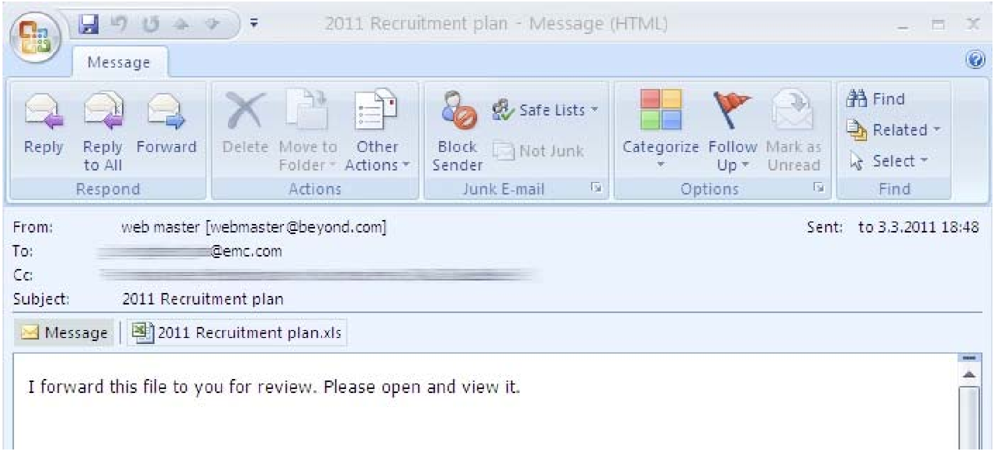
credit: jokeroo.com

Myth 7: Best to deal with cybersecurity at the end

- **Some forethought could save time,**
  - E.g., RSA (2011)

- **… effort …**
  - E.g., JP Morgan (2014)

- **… and expense.**
  - E.g., CurrentC (2014)



From: web master [webmaster@beyond.com]

Sent: to 3.3.2011 18:48

To: [redacted]@emc.com

Cc: [redacted]

Subject: 2011 Recruitment plan

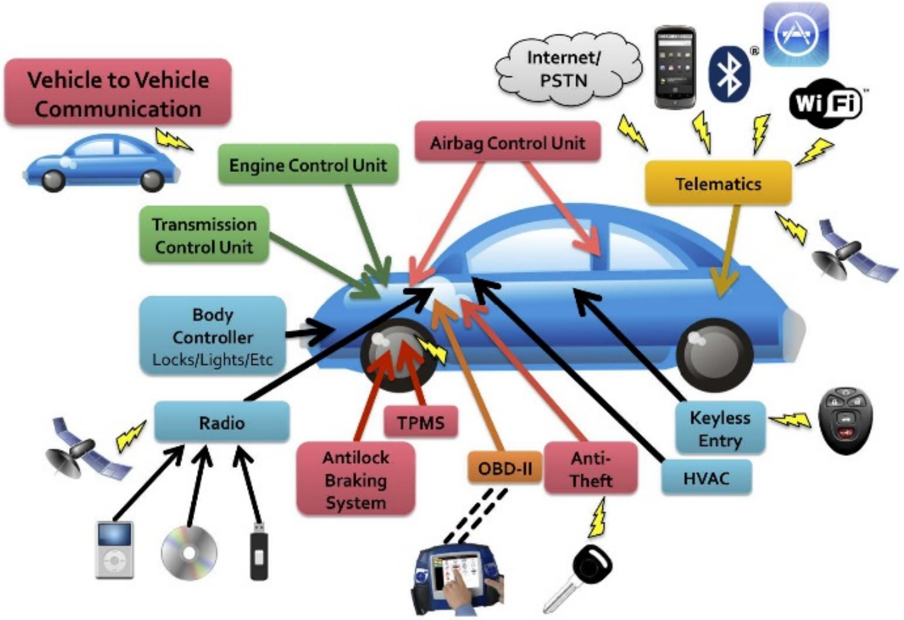
Message | 2011 Recruitment plan.xls

I forward this file to you for review. Please open and view it.

Credit: wired.com

Myth 8: Xxx machines don’t get viruses

- **If it has or relies on digital electronics, it’s susceptible.**
- **Examples:**
  - Cars, power plants, etc., Stuxnet (2010)
  - Cell phones, Linux devices, etc., XOR.DDoS (2015)
  - Web browsers



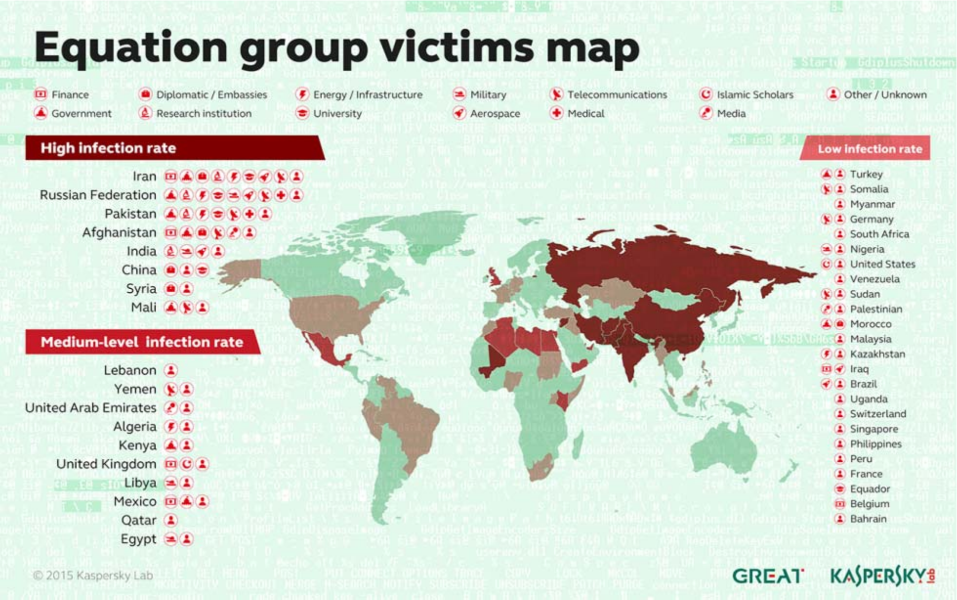
Credit: autosec.org

Myth 9: An APT is a hacker with a larger toolbox

- **An advanced persistent threat (APT) is:**
  - well-trained
  - well-resourced
  - capable of multi-year reconnaissance & attack campaigns
  - possibly can leverage intelligence tradecraft

- **APTs are thought to be government sponsored**

- **Equation Group (2015)**



See Cyber OT&E for more info!