Violations and Human Performance in Cybersecurity

Prof. Chris Johnson,
School of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson

Aim is to Provoke Discussion...

- Common software components into ATM:
  - networks, Linux, VOIP, SBAS...
- Human performance concerns everywhere:
  - Huge problems of competence – incl regulators;
  - Many conflicts between safety and security;
  - Inconsistent, inapplicable rules (lack of HF input);
  - Consistent, known violation of policies.
- Recommendations:
  - Act now these are violations NOT errors.

Aim is to Provoke Discussion...

- Recommendations:
  - Act now these are violations NOT errors.
- From a human factors perspective…
- Why are ANSPs waiting for the attack?

Paranoia?

- Many policies only exist on paper.
- Huge problem with complacency.
- “FAA ineffective in all critical areas including operational systems information security, future systems modernization security, management structure, policy implementation”.
- US Government Auditors Office

DoT Review of FAA CyberSecurity

DoT "unless effective action is taken quickly, it is likely to be a matter of when, not if, ATC systems encounter attacks that do serious harm to ATC operations."

“Attackers can take advantage of software vulnerabilities in commercial IP products to exploit ATC systems, which is especially worrisome at a time when the Nation is facing increased threats from sophisticated nation-state-sponsored cyber attacks"

Conflict Between Security and Safety

- Existing safety standards eg ED153
  - Focus on verification and validation;
  - In proportion to SWAL/criticality.
- Anti-viral systems violate ED-153:
  - Updated every 24-48 hours;
  - could themselves bring down ACC;
  - Cannot test anti-virus definiitons;
  - Without increasing security exposure.
- Do you want safety or security:
  - Can have both eg banking approach.

Vulnerabilities

- ‘Mass market’ viruses.
- You cannot disconnect the Internet.
  - Virtual channels from USB sticks.
- Contractors violate security policies:
  - My students take the systems to pieces…
- SESAR and NextGen scare me:
  - increasing traffic loads\systems integration

University of Glasgow

Some Recent Attacks….

- ANSP label on13 switches from eBay:
  - Flash memory for configuration data;
  - Not erased prior to sale;
  - ANSP have external disposal contract but…
- Used by sub-contractor at ACC:
  - Supervisor login for VLAN;
  - Upstream switch addresses/configs;
  - VTP trunk info and password;
  - SNMP community strings…

University of Glasgow

Some Recent Attacks…

- Regulator receives airprox radar data.
- ANSP and regulator use same player.
- ANSP ROM contains conficker.
- Regulator warns ANSP:
  - They claim player is obsolete anyway…
  - `no further investigation' at this time?

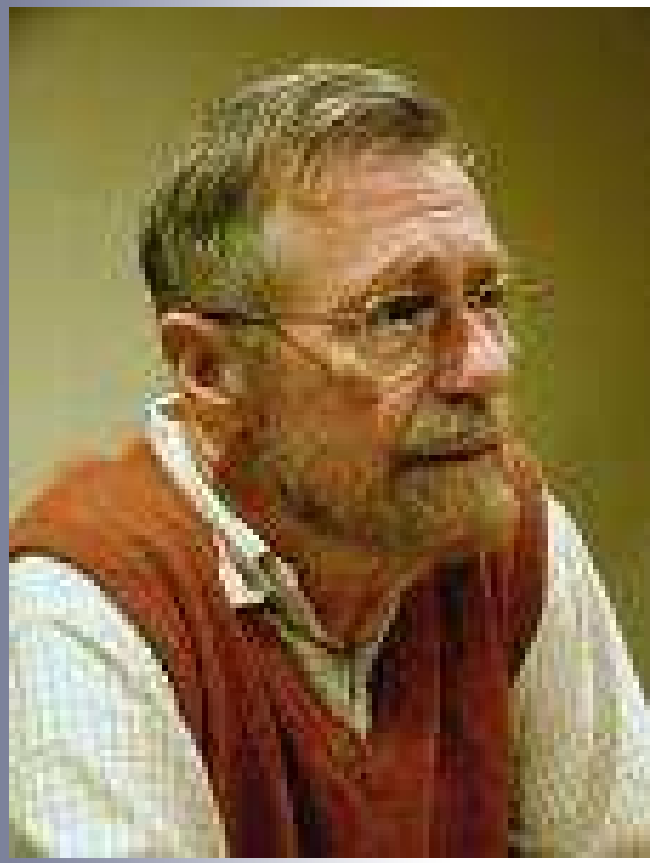
University of Glasgow

Some Recent Attacks

- Extortion attack .
- Sub-contractor:
  - Lack of background checks;
  - Corrupted the backups (not secure);
  - Waited 4 months then deleted primary copy.
- Bank asked for €2.5 million.

“Go But You Will Never Work Here Again…”

University of Glasgow



Edsger W Dijkstra (1930-2002)

Testing can prove the presence of errors, but not their absence.

W32.STUXNET, March 2010

- W32.Stuxnet multi-component malware
  - Attacks Programmable Logic Controllers (PLCs);
- Stuxnet has up to 4 zero-day exploits:
  - ATM very vulnerable to this…
  - Unusual range of languages (C/C++) team?
  - Used 2 legit Taiwanese digital signatures…
- Command & control servers identified:
  - Located in Malaysia and Denmark;
  - 155 countries, 40,000 IP addresses.

University of Glasgow

W32.STUXNET, March 2010

- Monitors frequency of attached
  - attacks systems operating 807-1210 Hz.
- Triggers a state machine to hide ‘sabotage’;
  1. Wait13 days;
  2. Set maximum frequency to 1410 Hz;
  3. Wait 27 days
  4. Set maximum frequency to 2 Hz;
  5. Set maximum frequency to 1064 Hz;
  6. Go to 1.
- Comparison with Dublin Airport.

W32.Duqu: C&C Breaking Firewalls

Corporate
Network

Operational
Network

University of Glasgow

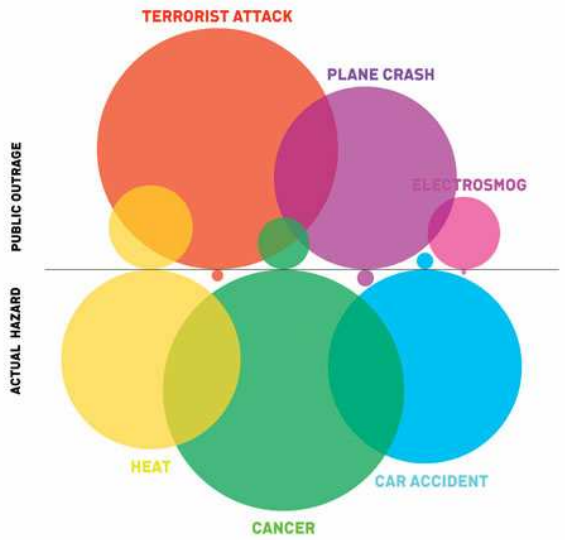
W32.Duqu

- Duqu will inject malware into:
  - Internet Explorer; Firefox;
  - Trend Micro PC-cillin AntiVirus Real-time Monitor.
- Checks for anti-viral products:
  - avp.exe, Mcshield.exe, avguard.exe, bdagent.exe, UmxCfg.exe, fsdfwd.exe, rtvscan.exe, ccSvcHst.exe, ekrn.exe, tmproxy.exe, RavMonD.exe.
- Extends Stuxnet to deal with Kaspersky…

University of Glasgow

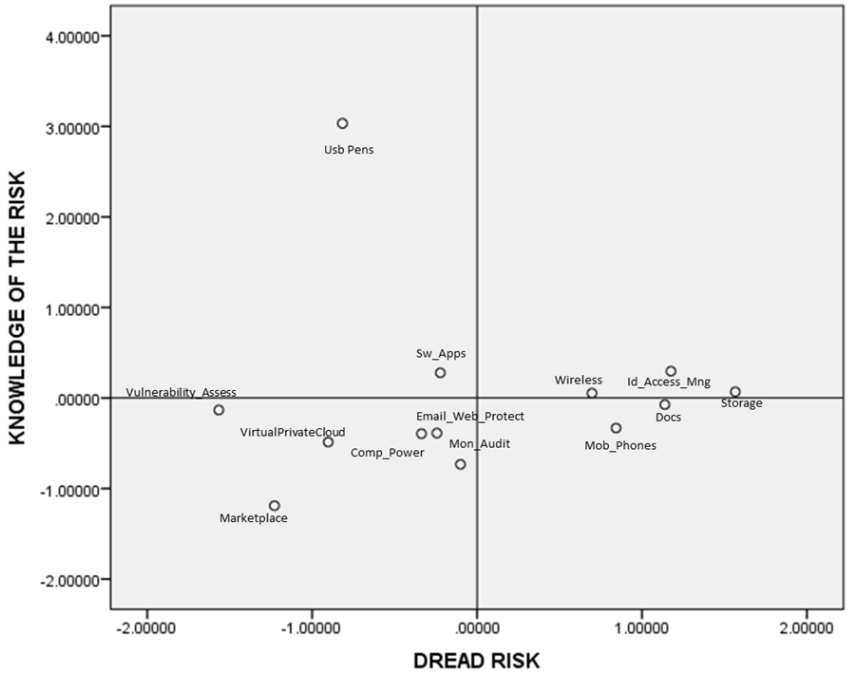
Forensics

Risk Perception and the Cloud



1. WHICH FACTORS INFLUENCE RISK PERCEPTION OF CLOUD COMPUTING?

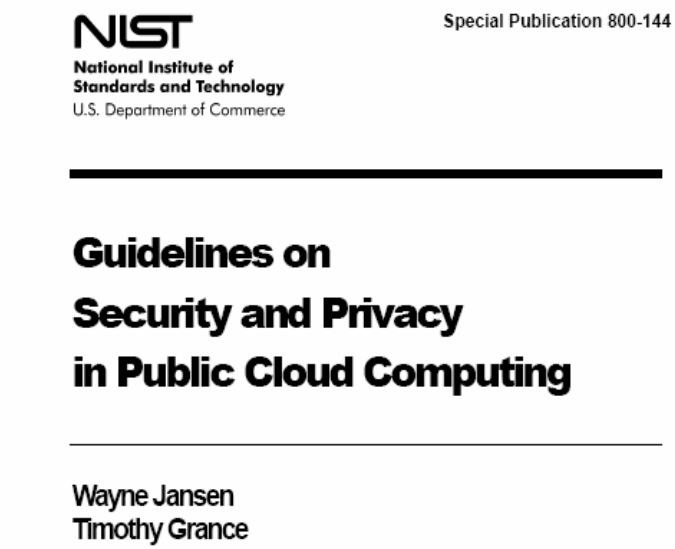
2. WHICH CLOUD SERVICES ARE PERCEIVED AS RISKY?



Gianfranco Elena, gianfrancoelena@gmail.com

University of Glasgow

Using the Cloud in ATM Engineering


NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-144

Guidelines on Security and Privacy in Public Cloud Computing

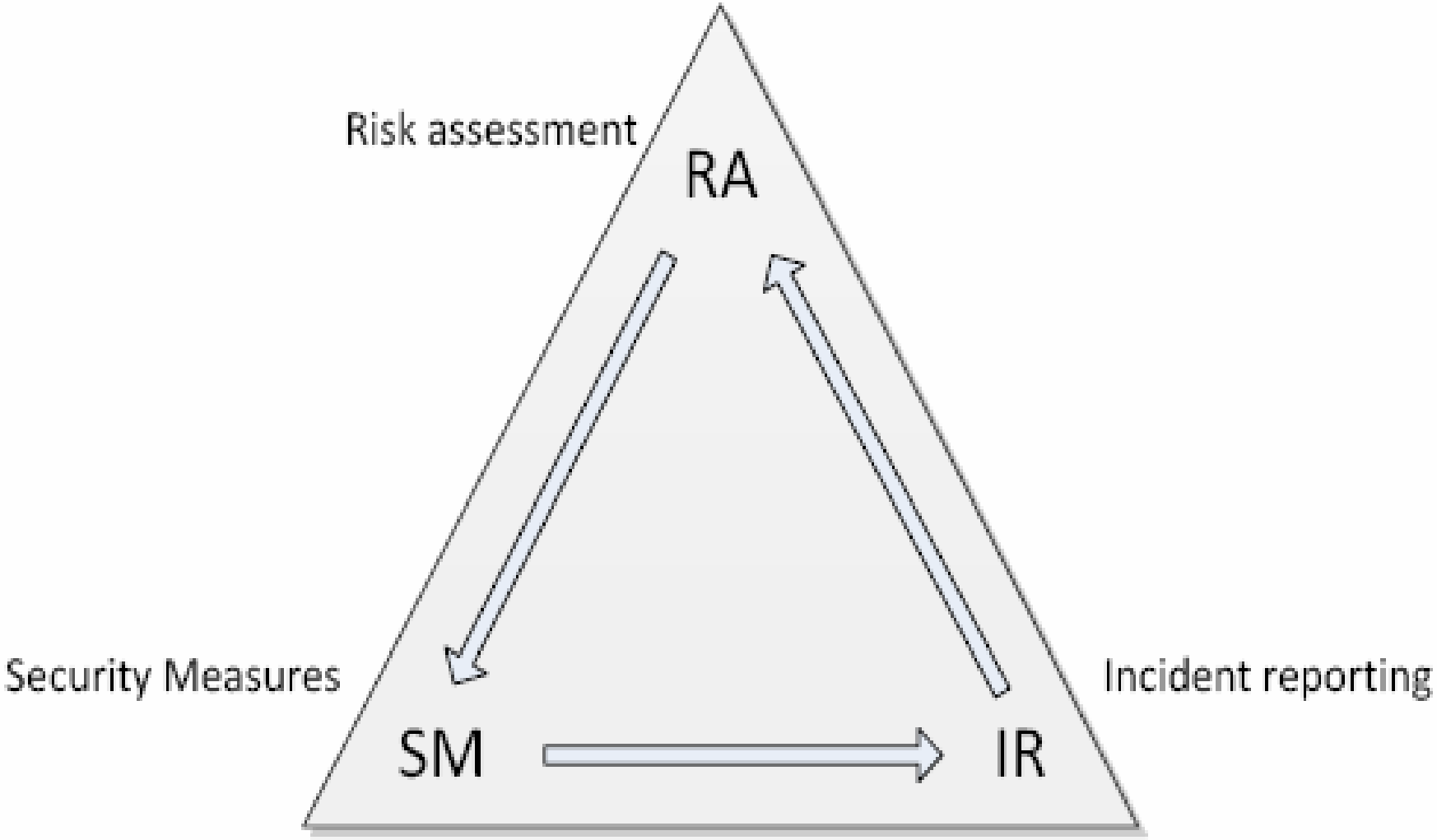
Wayne Jansen
Timothy Grance

- Security “Upside”:
  - Better coordination of security;
  - Better training and monitoring;
  - Share costs of secure infrastructure.
- Security “Downside”:
  - Providers unsure what is running;
  - Do all clients install secure patches?
  - What is ‘normal traffic’? Etc

http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909494

University of Glasgow

Security Governance Processes



University of Glasgow

Plans never survive contact with the Enemy

- So what can we do…

Future Issues: Proposed EC Directive

- Proposal for EC Cyber Security Directive:
  - Focus on ‘market operators’;
  - Europe wide mandatory reporting?
  - National Competent Authorities…
- 2013 Glasgow University with ENISA:
  - Supported by Google, Micorosoft, Amazon etc;
  - Develop incident reporting systems for Clouds;
  - What to report? Reduce burden on providers;
  - What information to share? Competition issues.

Future Issues: Cyber Insurance: 1st Party Risk

- *First party risk:*
  - Loss or damage to digital assets;
  - Business interruption;
  - Cyber extortion;
  - Reputational damage;
  - Theft of money and digital assets.
- Third party cyber risks:
  - Security and privacy breaches;
  - Investigation of privacy breach;
  - Customer notification expenses;
  - civil damages/defamation;
  - Loss of third party data.

Future Issues: Cyber Insurance

- Cloud services face a number of concerns.
- Most existing policies will not cover them.
- Lack of information:
  - About customer apps/ data (3rd party?);
  - Little actuarial data (incident reporting).
- “Cyber hurricane”:
  - Multiple claims in single incident destroy market?

The Future

- SESAR: Cybersec programme.
- FAA/NextGen/US Dept of Defence Project
- Impact of legislation uncertain…

University of Glasgow

Any Questions?