Author(s): Don M. Blumenthal, 2010

Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

PD-GOV **Public Domain – Government**: Works that are produced by the U.S. Government. (USC 17 § 105)

PD-EXP **Public Domain – Expired**: Works that are no longer protected due to an expired copyright term.

PD-SELF **Public Domain – Self Dedicated**: Works that a copyright holder has dedicated to the public domain.

(cc) ZERO **Creative Commons – Zero Waiver**

(cc) BY **Creative Commons – Attribution License**

(cc) BY-SA **Creative Commons – Attribution Share Alike License**

(cc) BY-NC **Creative Commons – Attribution Noncommercial License**

(cc) BY-NC-SA **Creative Commons – Attribution Noncommercial Share Alike License**

GNU-FDL **GNU – Free Documentation License**

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

PD-INEL **Public Domain – Ineligible**: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

© FAIR USE **Fair Use**: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

System Hacks and Attacks

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 5

Purposes

- Crime
- Malice/vandalism
- Glory within community
- Political terrorism – “hacktivism”
- Espionage
  - Nations or commercial interests
  - Nations against commercial interests
- State-state warfare
  - Some question its existence

Information Security Predictions

- Super Worms
  - Spread faster
  - More malicious
  - Mutate
- Exploit auto update features
- Attacks against routing or domain name structure
- Simultaneous cyber and physical attack

More *InfoSec* Predictions

- Stealthier malware
  - Polymorphic code
  - Anti-forensics
  - Tunnel
  - Kernel level root kits
  - Sniffing back doors
  - Sniffing PC activity; *e.g.,* keystroke logger
  - Reflected bounce attacks

Prescient

- InfoSec book on the mark for most part
  - Even where techniques didn't exist yet
- Fell short in understating
- Phishing existed
  - Targeted spear phishing, aimed at individuals
  - Whaling, aimed at upper executives
- E-blackmail (blackemail?)– pay or we'll wipe your computer

Not Addressed

- Organized crime has change landscape
  - Scale
  - Ability to wait to use stolen information
- Mules
  - Old term now used for people who accept shipments of goods bought with stolen info
- Range of frauds
- Proliferation of “bots” for sending spam and committing attacks

Critical Infrastructure (CII)

- Broader concepts than cybercrime
- Essential to minimal operations of government and economy
- Physical and electronic
- Countries define differently
- Consequential infrastructure if not CII
- All share dependency on computer based communications and control systems

Responsibilities

- Overall and individual categories help set lines of responsibility and communities of shared interest
- Public/private essential; private owns much of infrastructure
- Need to protect network, apps, OS, data

Framework

- Laws and regulations
- Government directives and policies
- Private and public standards and procedures

Considerations

- National security
- Economic security
- Public safety
- Duty to customers and shareholders

Processes and Methods

- Study that set concepts and drew attention
- Presidential designation of leadership
- Plan drafted after discussions with all affected sectors
- Legislation
- Information sharing
- Public education

Risks and Potentials

- "Newer" economies more at risk
  - Estonia uses Internet in economy much more than US
  - Much less brick and mortar backup
- Joint cyber-physical attack
  - Russia-Georgia

Proof Significant Issue

- Proof of sponsorship and even origin
- Some question if Estonia or cyber part of Russia-Georgia conflict were state sponsored
- Did Chinese government or private sector attack US/Google/*et al* recently
- June attacks on US and South Korea supposedly from North Korea may have come from London

US Reactions

- Cybercime statutes such as Computer Fraud and Abuse Act
- Federal and state statutes regarding information security and privacy
- Info warfare “live fire exercise” (official term) during Clinton administration
  - Similar exercises ongoing
- Permanent US Cyber Command established mid-2009

Recent Federal Activity

- Commission on Cybersecurity for the 44th Presidency
  - http://csis.org/program/commission-cybersecurity-44th-presidency
- Obama administration created cyber security czar position to coordinate agencies' activities

Pending Legislation

- S. 773 – Cybersecurity Act of 2009
  - Information gathering and coordination
  - Standards setting
  - Scholarships and competitions
- H.R. 4461 - Cybersecurity Enhancement Act of 2009
  - Similar but narrower on standards setting
- S. 1490 - Personal Data Privacy and Security Act of 2009 (discussed earlier)

Non-US Government Examples

- Council of Europe Convention on Cybercrime holds management primarily responsible when company targeted successfully
- Model cybercrime toolkit at http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

Private Sector

- Still has role
  - Tort
  - Contract
  - Shareholder
- Public education
  - By private or public sector