



Homeland
Security

Resilient Accord

Cybersecurity Overview

Understanding the Cyber Risk Landscape

Presented by:

Adam Bulava, NCCIC Cyber Planning and Exercise Program (CPEP)

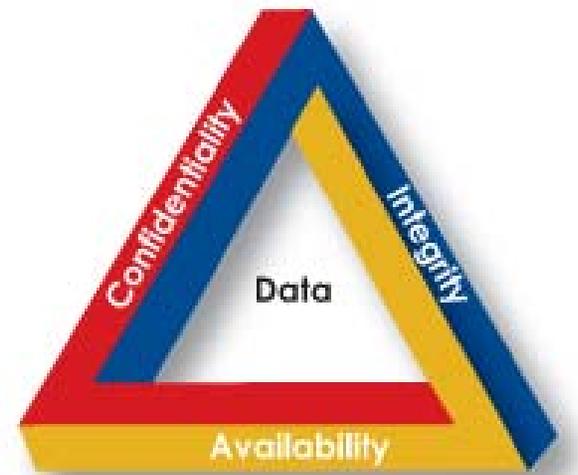
What is Cyberspace?

- The interdependent network of IT infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries
 - Defined in NSPD-54/HSPD-23
- Common usage of the term refers to the “virtual” environment of information and interactions between people



What is Cybersecurity?

- The protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users
- Safeguarding computer systems, as well as the data contained within, and maintaining:
 - Confidentiality
 - Integrity
 - Availability

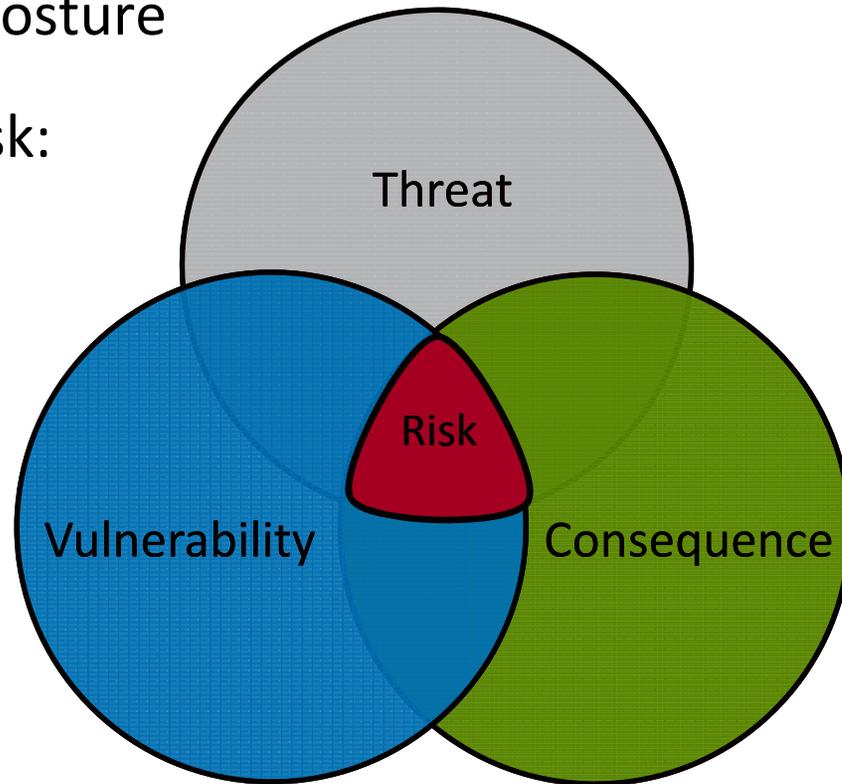


The Cybersecurity Challenge

- Cyber incidents are increasing in frequency, sophistication, and scale
- Cybersecurity in the news:
 - United States remains top targeted country for malicious activity
 - Cyber criminals are using new methods to steal credit card data
 - *Stuxnet* and *Stuxnet*-variants infect control systems
 - *Shamoon* malware able to “brick” computers
 - Internet-connected appliances confirmed as source of major spam attacks
- We can be doing more to prevent cyber incidents through understanding potential impacts and mitigating cyber risk

Examining Cyber Risk

- Calculating and mitigating cyber risk enhances your security posture
- Components of Cyber Risk:
 - Threat
 - Vulnerability
 - Consequence



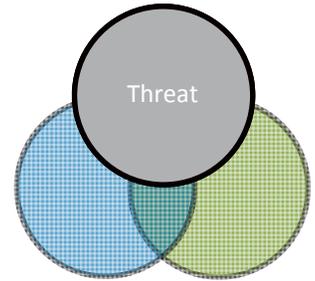
What type of cyber threats may impact your ability to perform essential functions?



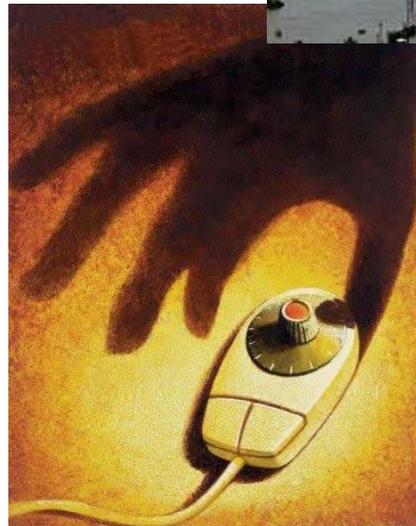
**Homeland
Security**

The Cyber Threat

- Threats that may impact your ability to perform essential functions come in various forms:
 - Natural Disasters
 - Accidents, Failures, and Human Error
 - Human Threat



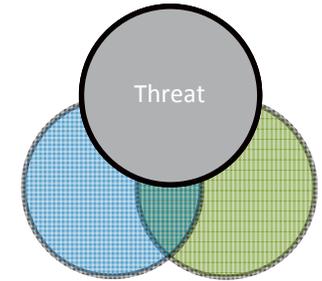
FIRE
Seattle data center fire knocks out Bing Travel, other Web sites
by Cook, Bishop on Friday, July 3, 2009, 7:07am PDT
52 Comments | [Permalink](#)
Bad news | Broadband | Business | Corporate IT | Web



Data center tenants carry servers out of Fisher Plaza this morning.

Cyber Threat: Human Threats

Who is behind these intentional threats?



- Bot-network Operators
 - Take over multiple systems
 - Coordinate attacks and distribute phishing schemes, spam, and malware attacks



- Criminals and Criminal Groups
 - Cyber-based attacks offer new means to commit traditional crimes, such as fraud and extortion
 - Organized cyber crime groups have adopted legitimate business practices, structure, and method of operation



- Foreign Intelligence Services
 - Cyber tools are part of information-gathering and espionage activities
 - Could affect the daily lives of U.S. citizens across the country



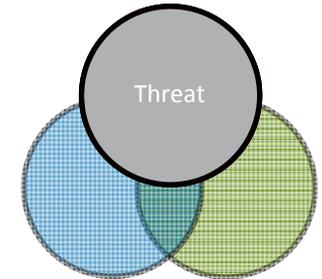
- Hackers and Script Kiddies
 - Hackers are more sophisticated and tools are easier to use
 - Script Kiddies – untrained hackers that find and exploit code/tools on the Internet and run them indiscriminately against targets



Homeland
Security

Cyber Threat: Human Threats

Who is behind these intentional threats?



- Insider Threat
 - Insiders have a unique advantage due to access/trust
 - They can be motivated by revenge, organizational disputes, personal problems, boredom, curiosity, or to “prove a point”



- Phishers
 - Individuals, or small groups who attempt to steal identities or information for monetary gain



- Spammers
 - Individuals or organizations who distribute unsolicited e-mail with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware, or attack organizations



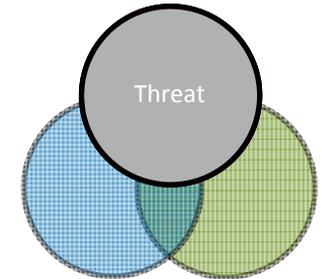
- Malware Authors
 - Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware

- Terrorists
 - Cyber attacks have the potential to cripple unsecured infrastructures
 - Cyber-linkages between sectors raise the risk of cascading failure



Homeland
Security

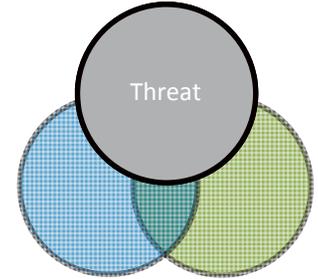
Cyber Threat: Malware



- Malware can be hosted on a malicious web sites, sent via email, or made to self-propagate across networks
- It can be used to steal information, destroy data, annoy users, or allow attackers to remotely control hosts
- Common types include:
 - Virus
 - Worm
 - Trojan



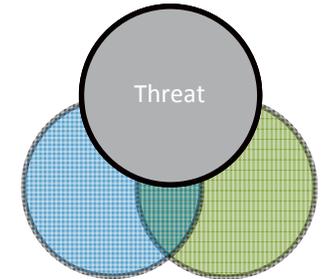
Cyber Threat: Denial of Service



- In a Denial of Service (DoS) attack, a hacker attempts to overload a service so that legitimate users can no longer access it
- Typical DoS attacks target web servers to make websites unavailable
- In a Distributed Denial of Service (DDoS) attack, hackers use a botnet to flood a web server with requests
 - Shift to high-bandwidth attacks from hosting centers, rather than compromised home computers or willing participants



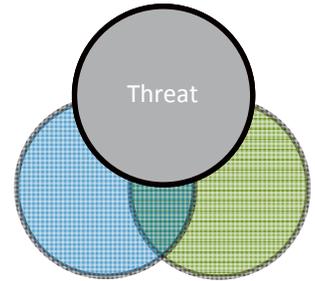
Cyber Threat Trends



- Threats are increasing because:
 - Hacking tools are more readily available and simpler to use
 - The potential impact of cyber attacks continues to grow
- Hacker motivation is changing:
 - No longer egocentric, hobbyist hackers seeking entertainment and internet status
 - Shift to professional cyber criminals motivated by money whose success relies on remaining undetected
- Inherently decentralized and open nature of the Internet continues to make cybersecurity difficult

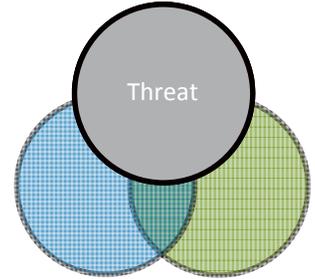
Hacking Tools are Easier to Use

FireSheep: Session Hijacking



Homeland Security

URL Shortening and QR Codes



Simplified by necessity, but be careful where you click!

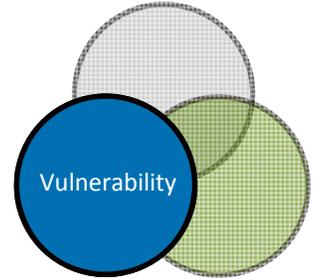
- With more and more content on the Internet, we have condensed and simplified our information through shortened URLs and 2D barcodes
- Below are two examples commonly found on social networking websites (where short web addresses are at a premium):

<http://bit.ly/ResilientAccord>



QR Codes can be scanned by most smart phones!

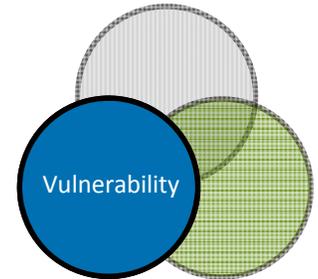
Cyber Vulnerabilities



- Security holes can render systems and networks susceptible to disruption, destruction, and exploitation
 - Implementing good security practices is difficult with increasingly interconnected networks
 - Fixing one vulnerability often opens up additional vulnerabilities
 - You are only as strong as your weakest link
- Technology moves faster than policy
 - Unpatched systems are low-hanging fruit for cyber attackers.
 - By implementing a policy for patching systems and servers, potential vulnerabilities and overall cyber risk are greatly reduced



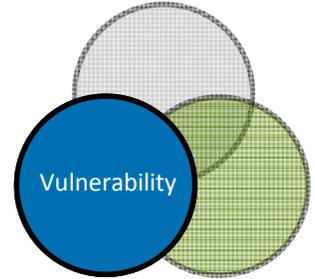
Cyber Vulnerability: Heartbleed



- Vulnerability in the widely-used OpenSSL encryption software
- Affects websites, email, instant messaging, and some virtual private networks (VPNs)
- Allows remote hackers to access sensitive data including
 - Usernames and passwords
 - Encryption keys
 - Protected content



Cyber Vulnerability Trends

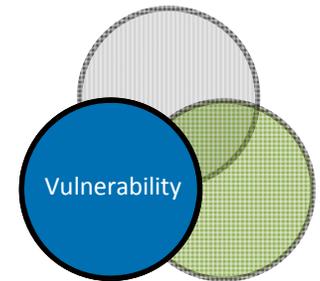


- We are fighting an uphill security battle:
 - The same vulnerabilities we see in the critical infrastructure community are transitioning to the home
 - Attackers are currently targeting vulnerabilities in new technologies and capitalizing on a lack of understanding
 - IPv6, Mobile, Social Media, Cloud Computing, etc.
 - Tech innovation driven by market that continues to focus on availability and interconnectivity, as opposed to security



Security Takes a Back Seat

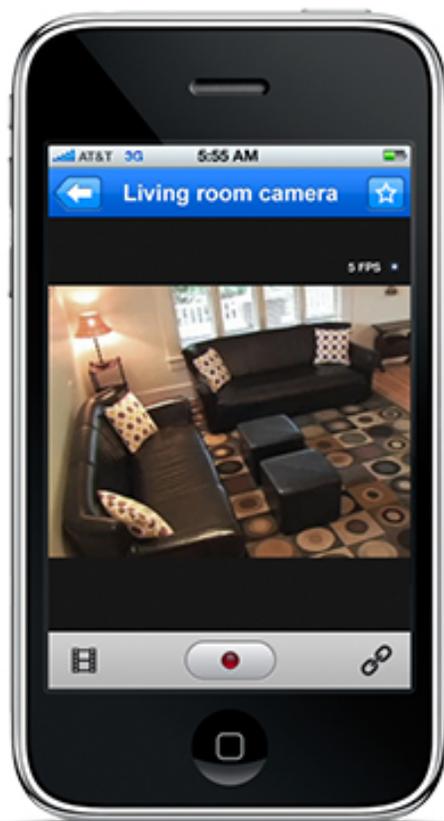
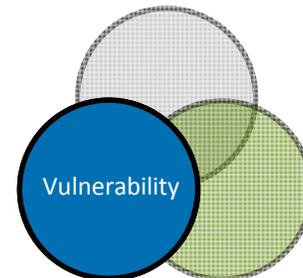
Mobile Applications Focus on Interconnectivity and Availability



Homeland
Security

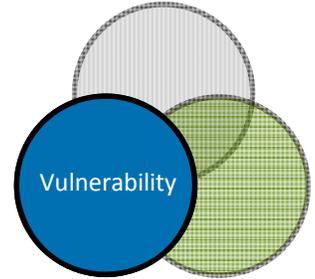
Mobile App Example

Controlling and Monitoring Remotely – Now for Your Home!



Homeland
Security

Another Mobile App Example



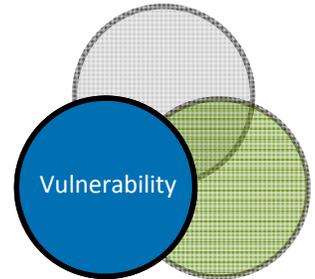
Near Field Communication (NFC)

- Enables
 - Mobile payments
 - Ticketing applications
 - Exchanging contact information
- Attack methods
 - Eavesdropping
 - Data modification
 - Relay attack



Homeland
Security

Value of Social Networking

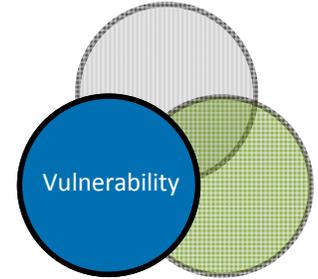


Does your organization use social networking websites and for what?



**Homeland
Security**

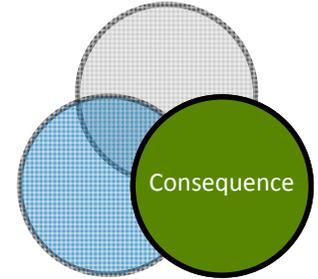
Value of Social Networking



- Carefully consider how your department or agency is using social networking websites such as Facebook and Twitter:
 - Spreading information by any means necessary is often a good approach, but if utilizing these sites for continuity and other critical messages, please consider the global audience
 - As more users become dependent on these as their information source, take into account what would happen if these information feeds were compromised and how easy they are to imitate



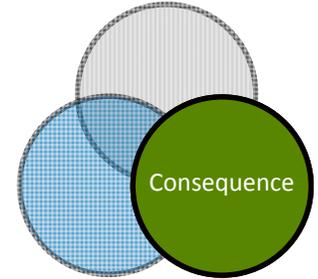
Cyber Consequences



- The effects of cyber attacks can be severe:
 - Cyber linkages among sectors raise the risk of cascading failures throughout the Nation during a cyber incident
 - The loss or degradation of certain critical infrastructure functions could negatively impact performance in other areas
 - Establishing continuity of operations plans and procedures mitigate consequences from cyber incidents and assure performance of essential functions



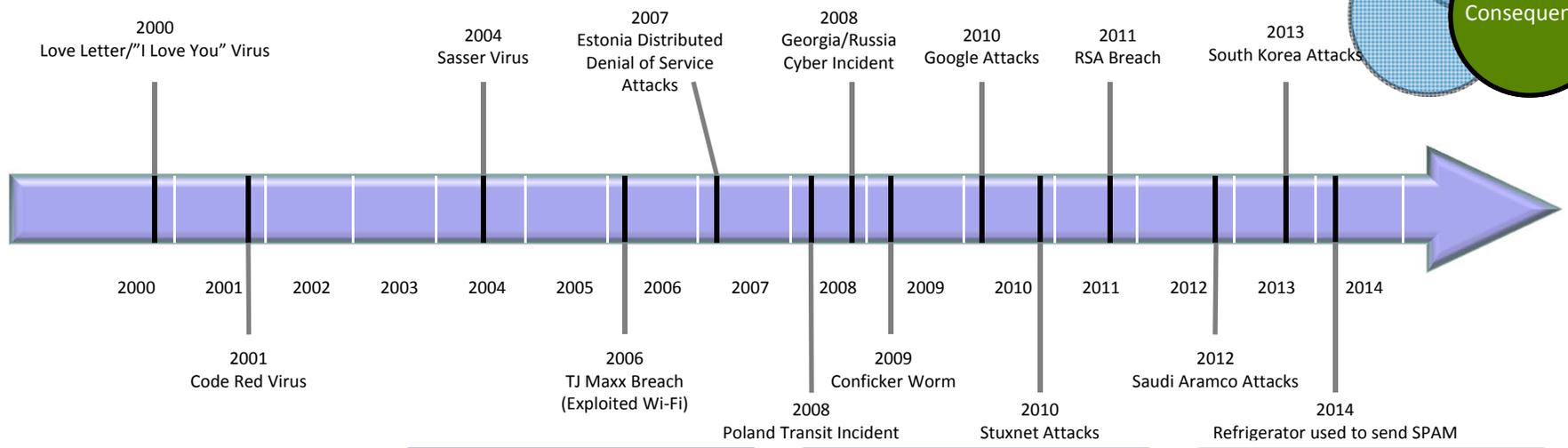
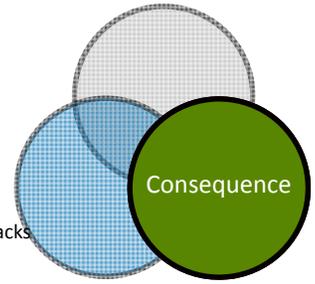
Cyber Consequence Trends



- Due to cyber linkages, it is becoming difficult to envision cyber-only consequences as a result of a modern cyber attack
- More communication and coordination is required than ever before during the response to cyber attacks:
 - Critical infrastructure attacks are becoming more common. The private sector owns over 80% of the critical infrastructure (and is often the first to detect a problem)
 - Planning and exercises can increase our ability to effectively respond to the wide-ranging consequences of a multi-sector cyber attack



Well-Known Cyber Incidents



1980-2000

- First virus emerges (1983)
- Morris Internet Worm (1988)
- Affected 10% of Internet's computers
- AOL Phishing Attacks (1995)
- Seeking passwords and credit card info
- Melissa Virus (1999)
- Love Letter Virus (2000)
- One of the biggest outbreaks of all time

2001-2006

- Blaster Worm (2003)
- Sasser Virus (2004)
- Choice Point Breach (2005)
- First breach of Personally-Identifiable Information (PII)
- VA Laptop (2006)
- 26.5 million veterans' data is compromised after a laptop is stolen
- TJ Maxx Breach (2007)
- Exploiting Wi-Fi
- Estonia DDoS (2007)

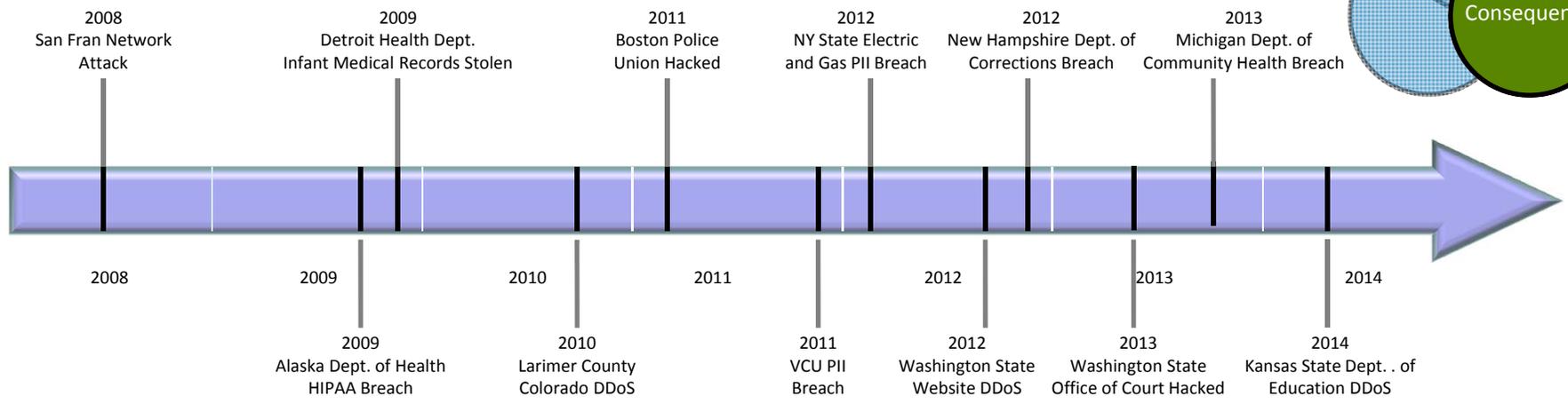
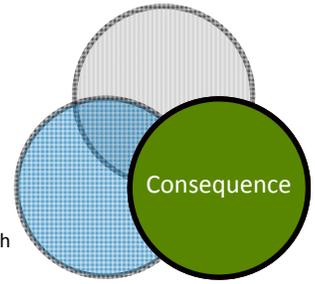
2006-2011

- Distributed Denial-of-Service attacks on Estonia
- Georgia-Russia Conflict (2008)
- Conficker Worm (2009)
- Required international coordination and response
- Stuxnet (2010)
- Targets control systems
- Epsilon Breach (2011)
- Sony PlayStation Breach (2011)
- RSA Breach (2011)

2012-Present

- Duqu (2011/2012)
- Flame (2012)
- Saudi Aramco (2012)
- DDoS on Finance Sector (2012-2013)
- South Korea Attacks (2013)
- Kaptoxa malware used in Target, Michaels, Neiman Marcus credit card theft (2013)
- Confirmed spam attack using IT connected refrigerator as source (2014)

Recent Cyber Incidents: States



2008-2009

San Fran govt. network takeover (July 2008)

- Insider makes himself the only admin

Alaska Department of Health and Social Services (Oct. 2009)

- \$1.7 mil HIPAA settlement after minor beach

Detroit Health Dept. (Dec. 2009)

- Flash drive with infant medical records stolen

2010-2011

Larimer County Colorado (Sept. 2010)

- DDoS against county government systems in retaliation for DUI prosecution

Boston Police Union (Oct. 2011)

- “Anonymous” takes down Police Union site

Virginia Commonwealth University (VCU) (Nov. 2011)

- PII from 176,000 exposed

2012

NY State Electric and Gas (Jan. 2012)

- PII from 2 million customers exposed

State of Washington (Apr. 2012)

- DDoS took down state government website

New Hampshire Dep. of Corrections (Aug. 2012)

- Inmates accessed corrections records from within prison!

2013 - Present

Washington State Admin Office of the Courts Hacked (Feb. 2013)

- Exposed 160K SSNs
- 1 Million drivers license numbers

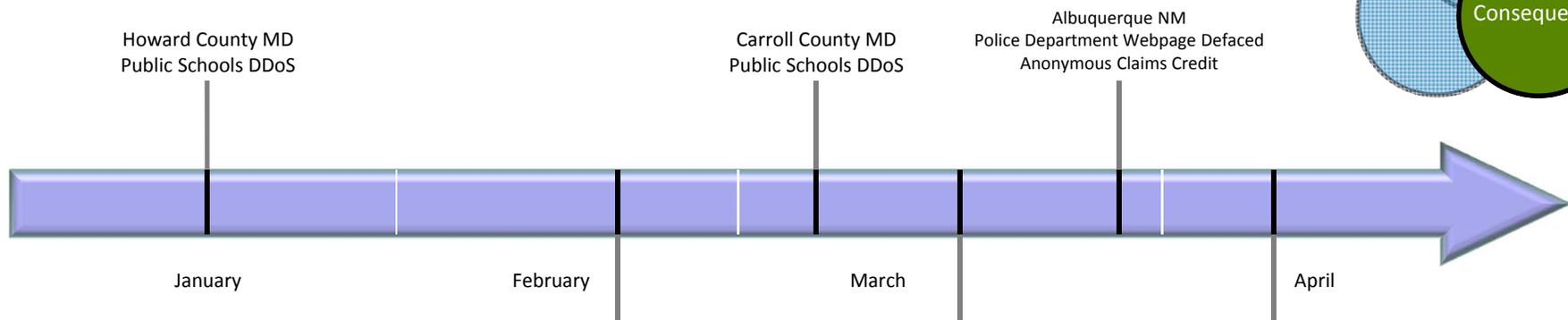
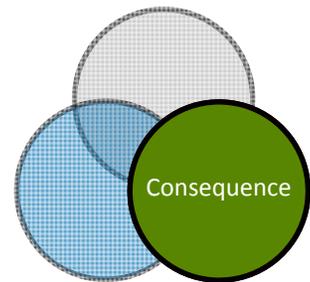
Michigan Dept. of Community Health (July 2013)

- 50,000 patient names, birth dates, SSNs

Kansas State Dept. of Education (Apr. 2014)

- DDoS shuts down annual math and reading tests

2014 Cyber Incidents: Local



Jan - Feb

Howard County, MD Public Schools DDoS attack

- System down one day

Medina County, OH

- Local Government operated community based internet, cable, and telephone services lost to DDoS
- 3500 residents affected over 10 hours
- Originated in Netherlands

March

Carroll County, MD Public Schools DDoS attack

- System down one day

Skagit County, WA

- Paid \$215K fine and agreed to Health and Human Services monitoring due to inadvertent release of protected health information
- Info incorrectly coded to go to a public facing server instead of a private server

Albuquerque, NM

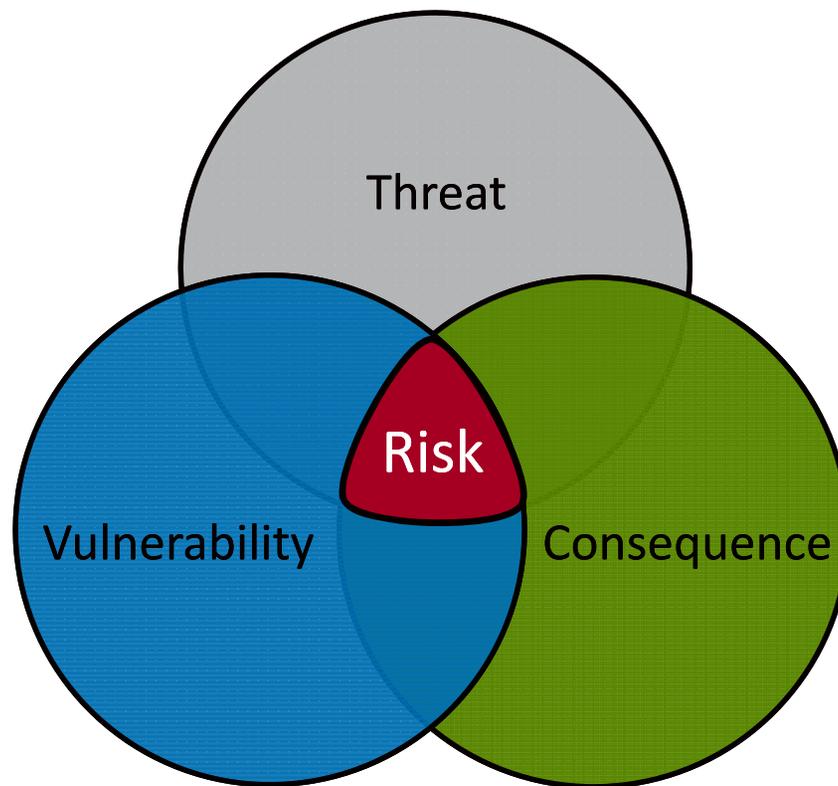
- Police Dept website defaced
- Anonymous claimed credit

April

Ector County, (Odessa) TX

- County Judge threatened by Anonymous Hacktivists due to ruling in child custody case
- Threatened cyber attacks against judge and his family Cincinnati, OH
- Baby Monitor Hacked
- Hacker exploited known vulnerability in camera firmware
- Typically used as a launch point for ID theft or malicious attacks
- Owners had not downloaded available patch

Cyber Risk Recap



Homeland
Security

Security is a Shared Responsibility

“If you own a dangerous old jalopy that can’t pass emission standards and you want to drive it around your private 10-acre field, that’s fine. But as soon as you take that unsafe car out onto the public road, you become a threat to others.”

Michael Barrett - Chief Information Security Officer, PayPal

“Linking our critical infrastructure to the Internet brings considerable benefits, but our daily reliance on this critical infrastructure means that we are vulnerable to disruptions in our ability to use it.”

Howard Schmidt – Former White House Cybersecurity Coordinator



Additional Resources

Website: DHS.gov/stopthinkconnect

Raises awareness on cybersecurity and provides helpful resources for public and private sector partners.

The screenshot shows the homepage of the Stop.Think.Connect website. At the top, there is a breadcrumb trail: Home > Get Involved > Stop.Think.Connect. On the left, a 'Get Involved' sidebar lists links for 'Citizen Corps', 'If You See Something, Say Something', 'Ready', and 'Stop.Think.Connect.'. The main content area features the title 'Stop.Think.Connect.' followed by a paragraph about the campaign's goal to increase understanding of cyber threats. Below this is a large graphic with a woman's face and the text 'ARE YOU SAFE ONLINE?' and 'Visit the online resource guide to find out'. Underneath the graphic is the text 'BROUGHT TO YOU BY DHS AND STOPTHINK.CONNECT.' and a section titled 'Get Involved and Informed' with four categories: 'National Network', 'Cyber Awareness Coalition', 'Academic Alliance', and 'Friends of the Campaign'. On the right, a 'Related Resources' sidebar lists links for 'Students', 'Parents and Educators', 'Young Professionals', 'Older Americans', 'Government', 'Industry', 'Small Business', and 'Law Enforcement'. Below that is a 'Spotlight' section for 'Stop.Think.Connect. Posters' with a poster image and a 'Download and distribute STC materials' link. At the bottom right, there is a 'Stop.Think.Connect. PSAs' section with a megaphone icon.



Homeland Security

Additional Resources (cont.)

Information Sharing: Multi-State Information Sharing & Analysis Center

- MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal, and territorial (SLTT) governments.
- The MS-ISAC 24x7 cyber security operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response.





Contact Us

Adam Bulava

DHS/NCCIC, CPEP

adam.bulava@hq.dhs.gov

703-235-5641

Cyber Planning and Exercise Program

DHS NCCIC

cep@hq.dhs.gov

703-235-3025



**Homeland
Security**



Homeland Security