



Homeland
Security

Understanding Cyber Risk at the 30,000 F00t-Level

Global Cyber Threats, Vulnerabilities, and
Consequences

Presented by:

Adam Bulava, DHS Cyber Exercise Program Support

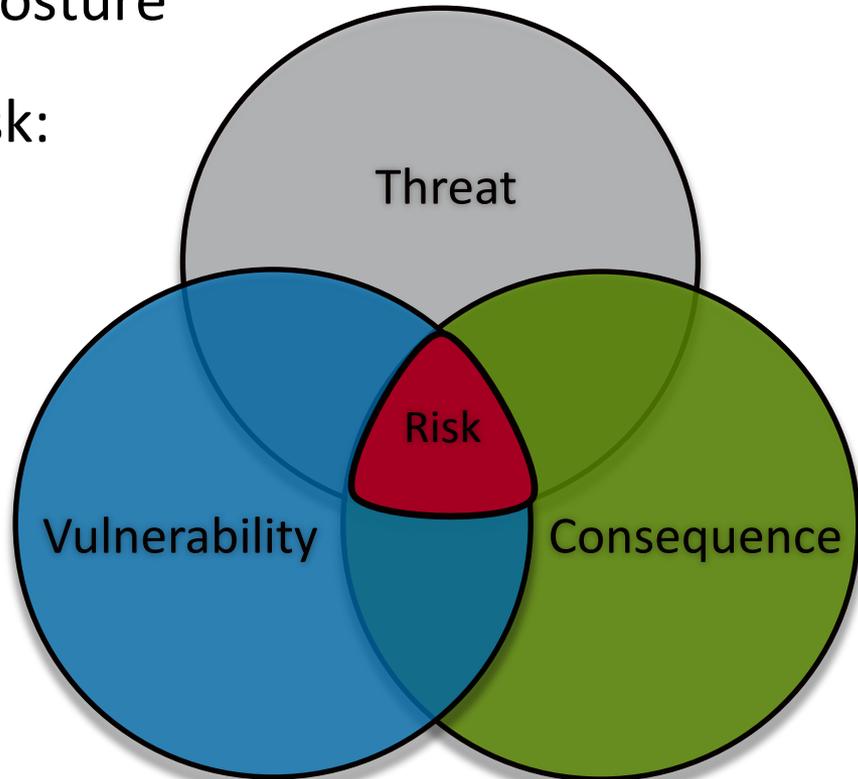
The Cybersecurity Challenge

- Cyber incidents are increasing in frequency, sophistication, and scale
- Cybersecurity in the news:
 - United States is the top targeted country for malicious activity
 - Government agencies ban USB devices after infections
 - *Stuxnet* and *Duqu* malware infect control systems
 - *Flame/Shamoon* most sophisticated cyber espionage weapons
- 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



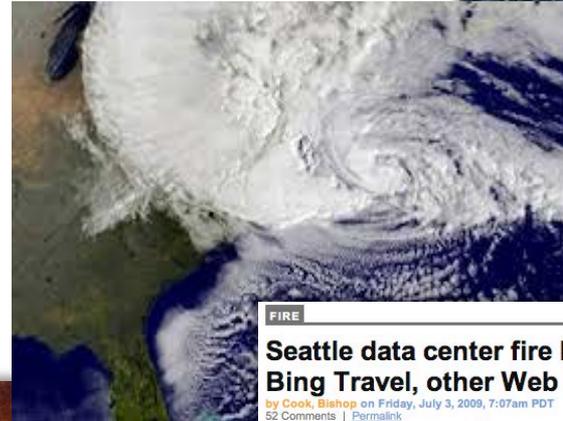
What types of cyber threats may impact your ability to perform essential functions?



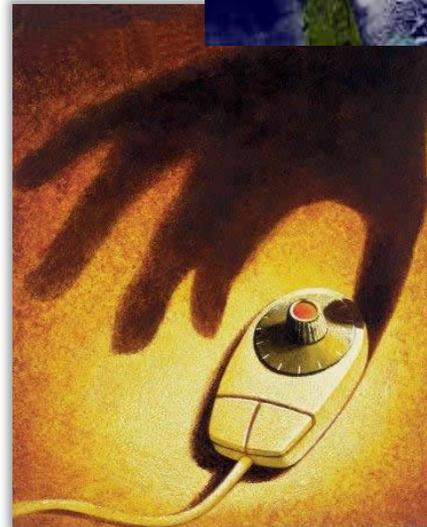
**Homeland
Security**

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 Threats



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](#)



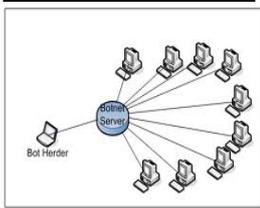
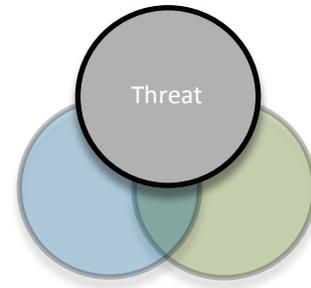
Data center tenants carry servers out of Fisher Plaza this morning.



**Homeland
Security**

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

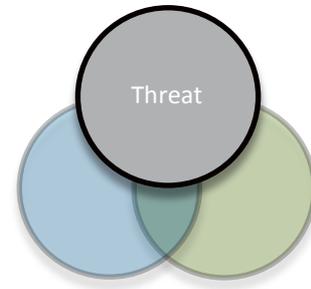
- Hackers are more sophisticated and tools are easier to use
- Script Kiddies – untrained hackers that find and exploit code/tools on the Internet and run them indiscriminately against targets



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

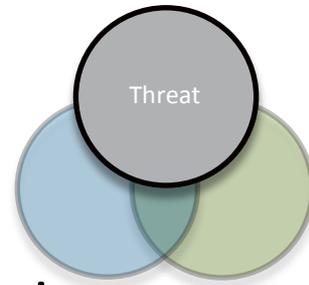
- Individuals or organizations with malicious intent carry out attacks against users by producing and distributing spyware and malware

- Terrorists

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



Homeland
Security

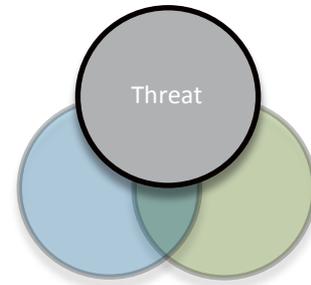


Cyber Threat: Malware

- 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 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



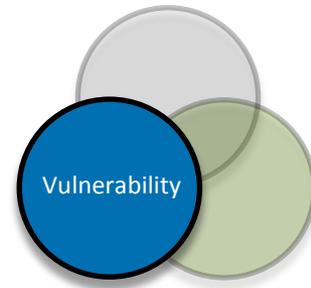
Cyber Vulnerabilities



- 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 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



Value of Social Networking



Does your organization use social networking websites? If so, for what purpose?



Value of Social Networking

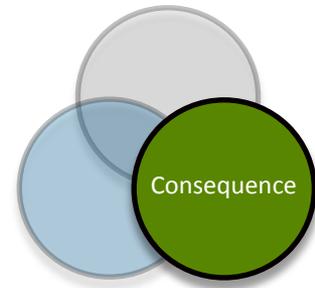


- Carefully consider how your department or agency is using social networking websites such as Facebook and Twitter:
 - Spreading information by any means necessary is often a good approach, but if utilizing these sites for continuity and other critical messages, please consider the global audience
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



Homeland
Security

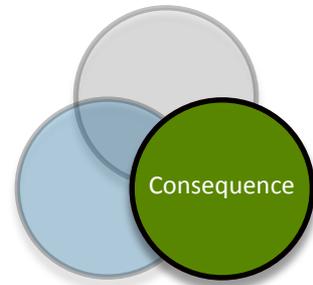
Cyber Consequences



- The effects of cyber attacks are 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 mitigates consequences from cyber incidents and ensures performance of essential functions



Cyber Consequence Trends

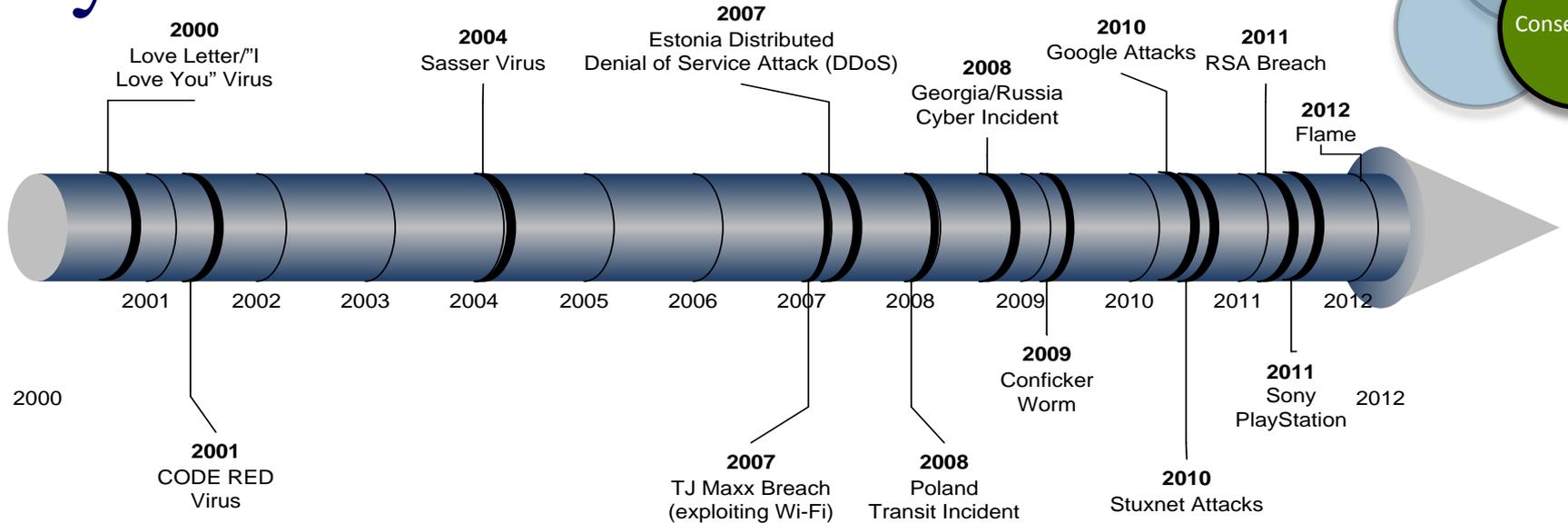
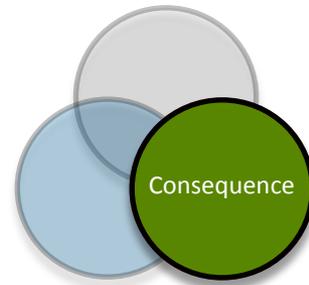


- Due to cyber linkages, it is becoming difficult to envision cyber-only consequences as a result of a modern cyber attack
- More communication and coordination is required than ever before during the response to cyber attacks:
 - Critical infrastructure attacks are becoming more common. The private 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



Homeland
Security

Cyber Incident Timeline: Global



1980-1999

- 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)

2000-2005

- Love Letter Virus (2000)
 - One of the biggest outbreaks of all time
- Blaster Worm (2003)
- Sasser Virus (2004)
- Choice Point Breach (2005)
 - First breach of Personally-Identifiable Information (PII)

2006-2009

- 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)
 - Distributed Denial-of-Service attacks on Estonia
- Georgia-Russia Conflict (2008)
- Conficker Worm (2009)
 - Required international coordination and response

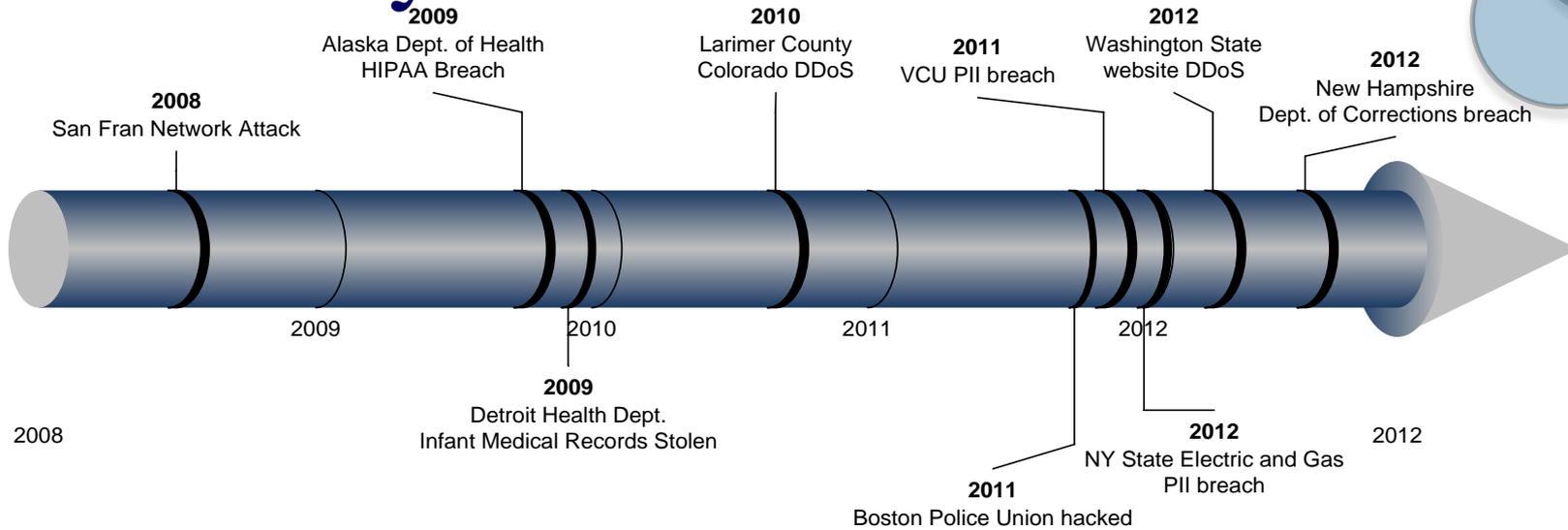
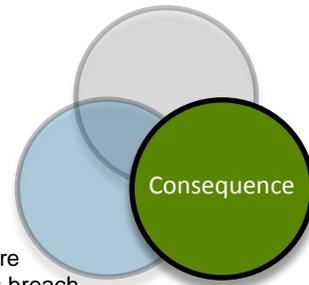
2010-Present

- Stuxnet (2010)
 - Targets control systems
- Epsilon Breach (2011)
 - World's largest provider of email marketing exposes customer data.
- Sony PlayStation (2011)
 - Targeted 77 million users
 - Network down 24 days
- RSA Breach (2011)
- Duqu (2011/2012)
- Flame (2012)
 - Most sophisticated cyber espionage tool



Homeland Security

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-Present

NY State Electric and Gas (Jan. 2012)

- PII from 2 million customers exposed

State of Washington DDoS (April 2012)

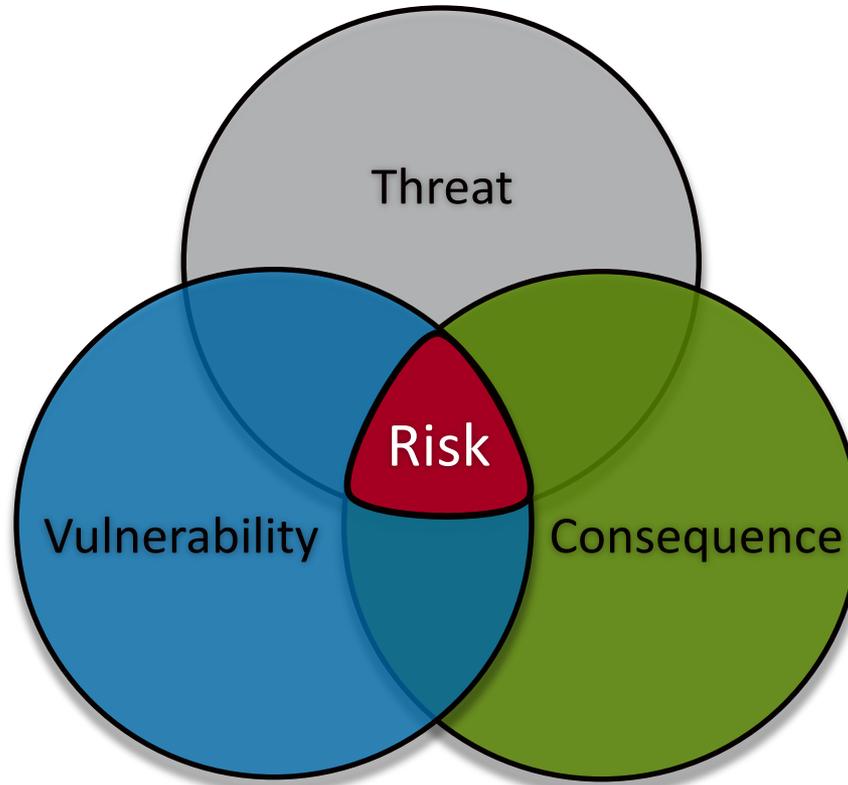
- Took down state government website

New Hampshire Dep. of Corrections (Aug. 2012)

- Inmates accessed corrections records from within prison!



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

“If we only protect the military networks and not the infrastructure, then we’ll have a great network that won’t be able to talk to anyone.”

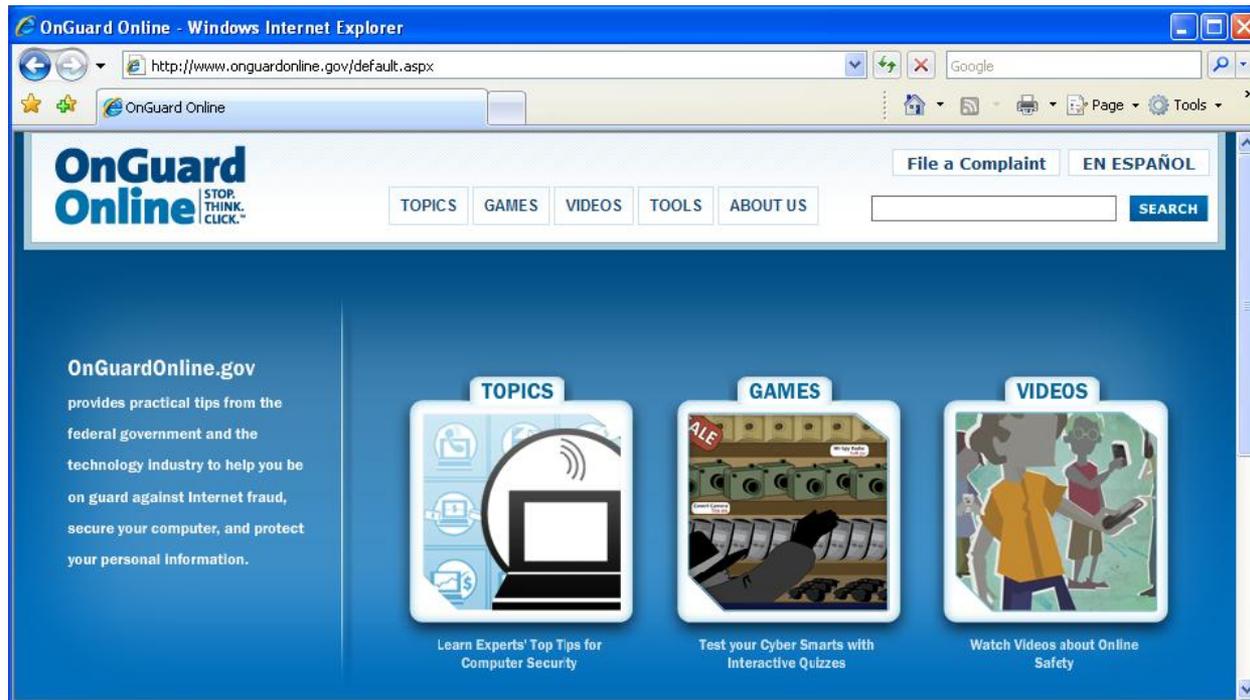
General Keith Alexander - Commander, US Cyber Command



Additional Resources

Website: OnGuardOnline.gov

Provides practical tips from the federal government and the technology industry to help you be on guard against internet fraud, secure your computer, and protect personal information

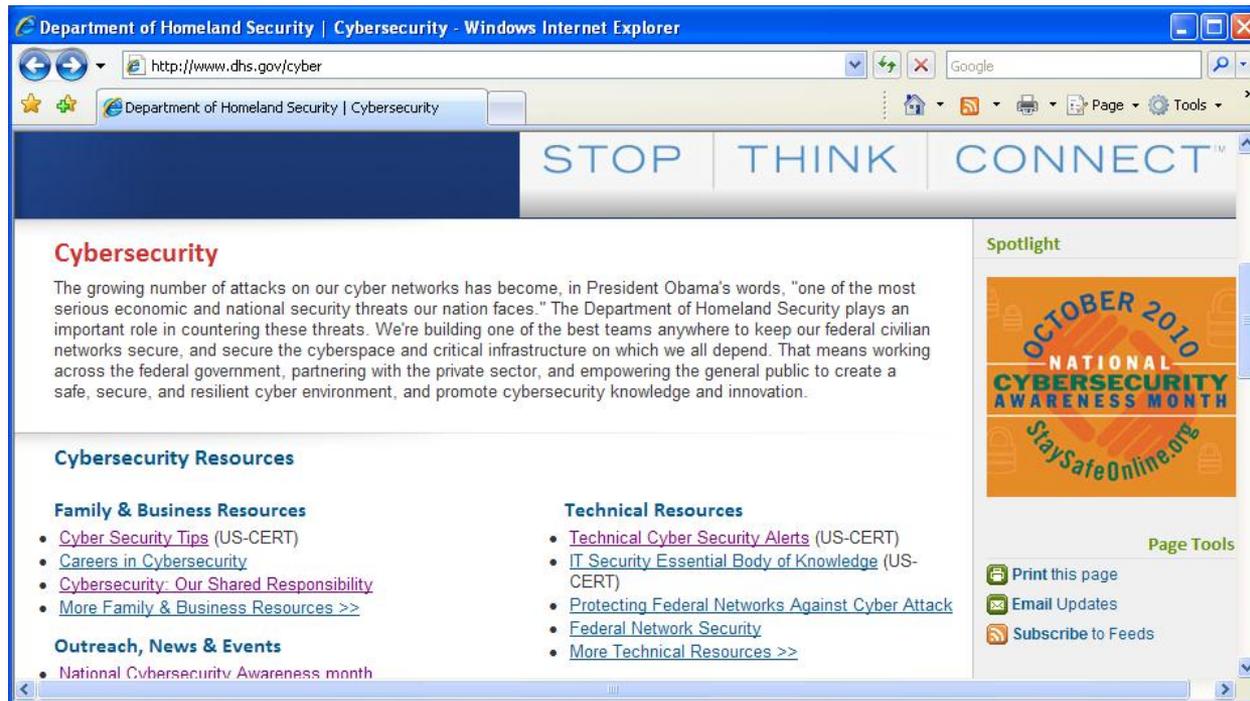


Homeland
Security

Additional Resources (cont.)

Website: DHS.gov/cyber

Provides more information about NCSD, U.S. Computer Emergency Readiness Team (US-CERT), and other groups and initiatives focused on cyber issues

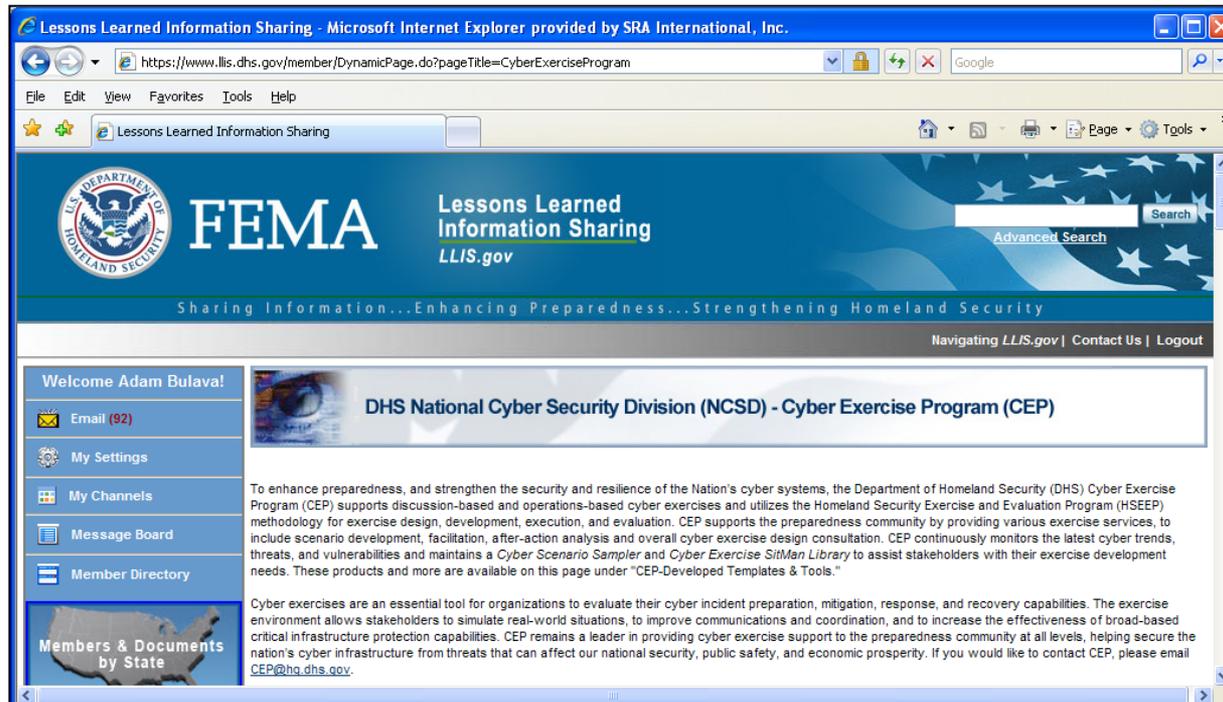


Homeland
Security

Additional Resources (cont.)

Website: [LLIS.dhs.gov](https://www.llis.dhs.gov) (available under “Partners” tab on LLIS homepage)

CEP-LLIS page provides numerous cyber exercise resources: after-action reports, sample scenario injects, SitMans and more. Available to all LLIS members. Visit [LLIS.gov](https://www.llis.dhs.gov) to find out how to become a member.



Homeland
Security

Any Questions?

CEP@DHS.GOV



**Homeland
Security**