2011 Federal Cybersecurity Conference and Workshop

Cybersecurity: Our Shared Responsibility

2011 Federal Cybersecurity Conference and Workshop

Sheraton Inner Harbor, Baltimore, MD

October 3-6, 2011

Table of Contents

Agendas **3**
October 3, 2011 3
October 4, 2011 3
October 5, 2011 5
October 6, 2011 6
Keynote Biographies **7**
Bobbie Stempfley 7
Dr. Lawrence A. Gordon 7
Howard A. Schmidt 8
Greg Schaffer 8
Teri Takai 9
Matt Coose 9
Keynote Presentation Summaries **10**
Bobbie Stempfley 10
Dr. Lawrence Gordon 11
Howard Schmidt 12
Greg Schaffer 12
Teri Takai 15
Matt Coose 16

2011 Fall Cybersecurity Conference and Workshop Agenda

October 3, 2011

9:30am – 12:00pm

Track A: Trusted Internet Connection (TIC) Working Group

Track B: Resiliency Management Model

Track C: Insider Threat

Track D: Shared Service Centers Symposium

1:30pm – 4:00pm

Track A: TIC Working Group: Part Two

Track B: Resiliency Management Model (Repeat)

Track C: Insider Threat

Track D: Shared Service Centers Symposium

October 4, 2011

8:00am – 8:15am

Opening and Welcome Remarks – Antione Manson, Program Manager of the Security Management Program, FNS

8:15am – 9:00am

Keynote – Bobbie Stempfley, Acting Assistant Secretary

9:15am – 10:30am

Track A: Digital Persona Protection

Track B: Managing Your Security Program: Anatomy of an Exploit

Track C: Cybersecurity Partnership: Teeing up the Issues

Track D: Future of FISMA: A Look at the Legislative Landscape

October 4, 2011 – Continued

<u>10:45am – 12:00pm</u>

Track A: Anti-Spearphishing Risks

Track B: Technologies for the Continuous Monitoring Domain

Track C: Infrastructure Protection: Securing Industrial Control Systems

Track D: The National Strategy for Trusted Identities in Cyber Space: How we Use HSPD-12

<u>1:15pm – 2:00pm</u>

Keynote – Dr. Lawrence Gordon

<u>2:00 – 3:15pm</u>

Track A: Risk and Resilience in the Age of the Advanced Persistent Threat

Track B: Getting the Most from your Network Security Technologies

Track C: Shared Service Centers

Track D: Continuous Monitoring and Policy Compliance: Cyber Scope and Future Capabilities

<u>3:30pm – 4:45pm</u>

Track A: The Intersection of the NIST Risk Management Hierarchy and the CERT Resilience Management Model (CERT_RMM)

Track B: Identity Management and Access Control in a New Cyber Landscape

Track C: Continuous Monitoring Working Group

Track D: Strategies for Risk Management: Can we Manage the Supply Chain Risk?

October 5, 2011

8:00am – 8:15am

Opening and Welcome Remarks – Antione Manson

8:15am – 9:00am

Keynote – The Honorable Howard Schmidt, Special Assistant to the President and Cybersecurity Coordinator

9:15am- 10:30am

Track A: Mobility: Using Commercial Mobile Devices

Track B: Cybersecurity Information Sharing – Moving Into the 21st Century

Track C: Top 10 U.S. Cyber Issues for R&D

Track D: National Initiative for Cybersecurity Education (NICE): Can we measure the health of the Cyber Workforce?

10:45am – 12:00pm

Track A: The Road Ahead: Cybersecurity Technology and The Human Factor

Track B: Where Cybersecurity and Mobility Meet

Track C: What is the National Framework Including Roles and Responsibilities?

Track D: What are the Policy Touch Points for Cloud Implementation?

1:15pm – 2:00pm

Keynote – Greg Schaffer, Acting DHS Deputy Undersecretary

2:00pm – 3:15pm

Track A: Insider Threat: Preventing and Detecting the Malicious Inside

Track B: Preventing Zero Day Attacks with Software Assurance

Track C: Cybersecurity for Secure Cloud Applications

Track D: SCRM: Leveraging Federal Best Practices

3:30pm – 4:45pm

Track A: Measuring and Managing Risks in Cyberspace

Track B: Tackling the Challenge of Advanced Persistent Threat

Track C: Sharing Best Practices: Mobile Risk Management and Hardware Boot Security

Track D: White House Initiatives on Federal Information Security

October 6, 2011

8:00am – 8:15am

Opening and Welcome Remarks – Matt Coose, Director of FNS

8:15am – 9:00am

Keynote – Ms. Teri Takai, CIO of the Department of Defense

9:15am – 10:30am

Track A: Red Teaming: The Business Case for Benefits and Penetration Testing

Track B: DNSSEC Implementation

Track C: Cyber Exercises Across Government: Executive Overview

Track D: International Information Sharing: What is the Status and Implications of our Data for Cloud Services?

10:45am – 12:00pm

Track A: Cyber Exercises Across Government: Executive Overview

Track B: Email Authentication

Track C: Cybersecurity Acquisition Lifecycle

Track D: Policy Wrap-up: Looking to the Future

12:00pm – 1:00pm

Closing Ceremonies – Matt Coose

Keynote Biographies

Bobbie Stempfley is the Acting Assistant Secretary of the Office of Cybersecurity and Communications, where she plays a leading role in developing the strategic direction for all of CS&C and its components, consisting of the National Cyber Security Division (NCSD), the Office of Emergency Communications (OEC), and the National Communications System (NCS). Prior to this position, Ms. Stempfley was the Acting Deputy Assistant Secretary of CS&C and the Director of the National Cyber Security Division.

Prior to her work in CS&C, she served as the Chief Information Officer of a major Department of Defense Agency, Defense Information Systems Agency (DISA), where she was responsible for supporting the Director in decision making; strategy development and communicating that strategy both internally and externally; aligning DISA program execution with Department of Defense (DoD) strategy for planning, engineering, acquiring, fielding and supporting global-net-centric solutions; operating the Global Information Grid (GIG); information assurance; and management of DISA information technology resources.

Dr. Lawrence A. Gordon is the Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance at the Robert H. Smith School of Business. He is also an Affiliate Professor in the University of Maryland Institute for Advanced Computer Studies. Dr. Gordon earned his Ph.D. in Managerial Economics from Rensselaer Polytechnic Institute. An internationally known scholar in the areas of managerial accounting and cybersecurity economics, Dr. Gordon's research focuses on such issues as economic aspects of information security, corporate performance measures, cost management systems, and capital investments. He is the author of more than 90 articles and several books.

Dr. Gordon's current research emphasizes the importance of utilizing concepts from managerial accounting and economics within an information-based economy. In particular, he is considered one of the pioneers in the emerging field of cybersecurity economics. Prior to joining Maryland, Dr. Gordon was a faculty member at McGill University and the University of Kansas. He also served as a Visiting Scholar at Columbia University while on sabbatical from Maryland.

Howard A. Schmidt has had a long distinguished career in defense, law enforcement and corporate security spanning more than 40 years. He brings together talents in business, defense, intelligence, law enforcement, privacy, academia and international relations through his distinguished career. He currently is Special Assistant to the President and the Cybersecurity Coordinator for the Federal Government. In this role Mr. Schmidt is responsible for coordinating interagency cybersecurity policy development and implementation and for coordinating engagement with Federal, state, local, international, and private sector cybersecurity partners.

Previously, Mr. Schmidt was the President and CEO of the Information Security Forum (ISF). Before ISF, he served as Vice President and Chief Information Security Officer and Chief Security Strategist for eBay Inc. He also served as Chief Security Strategist for the US-CERT Partners Program for the Department of Homeland Security. Before eBay, he served as the Vice Chair of the President's Critical Infrastructure Protection Board and as the Special Adviser for Cyberspace Security for the White House.

Greg Schaffer was named Acting Deputy Under Secretary for the National Protection and Programs Directorate (NPPD) on June 5, 2011. Prior to that appointment, Mr. Schaffer served as Assistant Secretary for Cybersecurity and Communications (CS&C), a position he had held since June 1, 2009, when he was appointed by U.S. Department of Homeland Security (DHS) Secretary Janet Napolitano. As Assistant Secretary, Mr. Schaffer worked within NPPD to lead the coordinated efforts of CS&C and its components, including the National Cyber Security Division, the Office of Emergency Communications and the National Communications System. He engaged the public and private sectors as well as international partners to prepare for, prevent, and respond to catastrophic incidents that could degrade or overwhelm the Nation's strategic cyber and communications infrastructure.

Before joining the Department, Mr. Schaffer served as Senior Vice President and Chief Risk Officer for Alltel Communications LLC, where he had responsibility for logical security, physical security, internal and external investigations, fraud, law enforcement relations, privacy and regulatory compliance.

Teri Takai is the Department of Defense Chief Information Officer (DoD CIO). She serves as the principal advisor to the Secretary of Defense for Information Management/Information Technology and Information Assurance as well as non-intelligence Space systems, critical satellite communications, navigation, and timing programs, spectrum and telecommunications. She provides strategy, leadership, and guidance to create a unified information management and technology vision for the Department and to ensure the delivery of information technology based capabilities required to support the broad set of Department missions.

Ms. Takai previously served as Chief Information Officer for the State of California. As a member of the Governor's cabinet, she advised the Governor on the strategic management and direction of information technology resources as the state worked to modernize and transform the way California does business with its citizens. Prior to her appointment in California, Ms. Takai served as Director of the Michigan Department of Information Technology (MDIT) since 2003, where she also served as the state's Chief Information officer.

Matt Coose is the Director of Federal Network Security (FNS) for the National Cyber Security Division (NCSD) of the Department of Homeland Security within the National Protection and Programs Directorate (NPPD). The FNS program works across the federal government to improve cybersecurity posture by monitoring and measuring capabilities, assessing gaps, influencing policy and strategy, and driving implementation of risk mitigation efforts. He was recently appointed to a senior OMB Task Force to develop cybersecurity metrics to be reported by all Federal agencies starting in 2010. He also chairs the Federal Systems Security Governance Board (FSSGB), providing guidance to the Information Systems Security Line of Business (ISSLOB), a joint OMB and DHS strategic sourcing body for cybersecurity related acquisitions.

Mr. Coose has over 19 years of leadership and management experience in both the federal and private sectors and has held a variety of positions in both business and information technology, including Aviation Officer in the U.S. Army, Six Sigma Consultant at General Electric, Program Manager at UUNET, Director of Managed Services Operations at OneSoft Corporation, and E-Commerce Branch Manager at the U.S. Department of Treasury.

Keynote Presentation Summary

Bobbie Stempfley

October 2011 Federal Cybersecurity Conference and Workshop and NCSAM theme is Cybersecurity: Our Shared Responsibility

- Need for public-private partnership

DHS mission

- Secure the dot-gov domain
- Work with the private sector to improve security of the dot-com domain

DHS Initiatives underway to accomplish mission

- Improved Federal Information Security Management Act (FISMA) implementation
- Trusted Internet Connections (TIC)
- Einstein program
- National Cybersecurity and Communications Integration Center (NCCIC)
- Onsite technical support for both Federal and non-Federal partners
- U.S. Computer Emergency Readiness Team (US-CERT)
- Industrial Control Systems CERT (ICS-CERT)

Partnerships/Collaboration/Information Sharing

- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- DHS and Department of Defense (DoD) memorandum of understanding (MOA)
- National Cybersecurity Division (NCSD) information sharing pilot with DoD Defense Cyber Crime Center and the Financial Services ISAC
- Cybersecurity Partners Local Access Plan (CPLAP)

Cyber Awareness Activities

- October 1st marked the beginning of the 8th annual National Cyber Security Awareness Month
- Theme is “Our Shared Responsibility”
- Stop.Think.Connect. campaign launched to engage audiences outside of cybersecurity professionals
- Information available at www.dhs.gov/cyber

Dr. Lawrence Gordon

Economic Impact of Cybersecurity Breaches on Corporations

- Cybersecurity breaches are a key concern to private and public sector organizations
- President Obama's initiatives
- Economic costs of cybersecurity breaches
- Conventional wisdom
- Need to consider implicit and explicit costs
- Key studies have reviewed the impact of breaches on Stock Market Returns (SMR)
- Large percentages of corporate breaches do not have a significant impact on firms
  - Customers and stockholders have become tolerant of breaches
  - Many firms have strengthened their remediation activities, thereby substantially reducing the cost of an average breach
- Breaches that do have a significant impact on SMR could threaten a firm's survival

Making Cybersecurity Investment Decisions

- Making the business/economic case
- Net Present Value (NPV) model
- Gordon- Loeb model derives optimal amount to invest (Need to consider security breach function [i.e., vulnerabilities, threats, and productivity of investments] & potential loss)
- Option value of investments
- Optimal level of information security investment
- Does not always increase with the level of vulnerability
- For a wide range of circumstances, firms should Invest ≤ 37% of expected loss
- Wait-and-see approach is often rational from an economics perspective due to real options

The Effect of Voluntarily Disclosing Cybersecurity Activities on Firm Value

- Voluntary disclosures concerning information security, in annual reports filed with the SEC, were found to be positively associated with increases in the stock market value of firms.

Cybersecurity Insurance: A Risk Transfer Mechanism

- Cybersecurity insurance as a mechanism to transfer risk
- Organization's perspective
- Assess if cybersecurity insurance is needed
- Evaluate available insurance policies
- Select appropriate policy and transfer risk
- Insurance company's perspective
- Pricing decisions require more actuarial data
- Adverse selection
- Moral hazard

- Slow to gain momentum

Cybersecurity Risk

- Uncertainty of potentially harmful events related to cybersecurity

Cybersecurity Risk Management

- Process of managing (reducing) potentially harmful uncertain events due to the lack of effective cybersecurity

Howard Schmidt

Administration Cybersecurity Priorities

1. Continuous monitoring
    - Know *what is on* your network
2. Trusted Internet Connections and Einstein
    - Know *what is entering and exiting* your network
3. Identity Management
    - Know *who is on* your network

Priority 1: Continuous Monitoring

- It covers a range of activities.
    - Asset inventory, system configuration, vulnerability assessment, automated reporting, and risk evaluation.
- Automated reporting
    - Tracking cyber incidents and cybersecurity progress shouldn’t be an exercise in paperwork. Therefore all of the tools that enable continuous monitoring should enable automated reporting.
    - The reports can form a baseline for future improvements and demonstrate progress on the problem.
- Risk evaluation
    - Risk evaluation is how you use the data from continuous monitoring to change behavior.
    - Use data feeds to evaluate overall risk at component and agency level.
    - Show people at the component level what their risk score is and what actions they can take to lower that score.

    - By converting many different weaknesses into a single risk score, you help component-level system administrators prioritize their time: I have 5 things on my to-do list and only have time to do 3. Which 3 should I do?
    - Risk evaluation and the resulting dashboards should make the answer to this question simple for a component-level system administrator.
    - They should see, here is one missing patch that is contributing the most to my risk score, so I'm going to get that patch installed.
- Continuous monitoring is the baseline and foundation of our entire security effort.

Priority 2: Trusted Internet Connection Initiative and Einstein Programs

- Know where all of your entry and exit points are for the network.
    - We've been working to minimize these points across the Federal government. Then focus our security at those gateways to implement sensors and security controls.
- Benefits:
    - Common Operating Picture & Situational Awareness
    - Identify cross-agency threats
    - Piece together information that is obscured at the individual agency level
    - Efficiencies: single gateway at which to implement security measures like Einstein 2, intrusion detection system
    - Government-wide security controls
- This effort isn't something agencies have to undertake by themselves. GSA has certified several private sector companies under a program known as Managed Trusted Internet Protocol Services (MTIPS), which are private internet service providers that serve federal agencies, to provide TIC services.
- In conjunction with the TIC initiative, the EINSTEIN system is designed to provide the U.S. government with an early warning system for intrusions to Federal Executive Branch civilian networks.

Priority 3: Identity Management

- **Implementation**: HSDP-12 mandates Personal Identity Verification (PIV) cards for both physical and logical access, and it outlines a process for vetting and issuance.
- Currently focusing on a single metric: the percentage of agency user accounts that require the use of PIV cards for logging onto the network.
- By requiring that users' login with their PIV cards, agencies will know who is on their networks.

- The next step is to enable systems and web applications to accept PIV authentication. Agencies need to be working on that, but it will take time.
- In the short term, there is no excuse: agencies should be requiring the majority of their users to login only with their PIV cards. We have the cards, now let's use them.

Greg Schaffer

Threats intensify in frequency and persistence day in and day out

White House Legislative Proposal

- The White House in May released a legislative proposal aimed at streamlining the Federal government's cyber coordination and effectiveness.
- The proposal would:
  - *Solidify DHS's responsibility for leading the protection of Federal civilian networks*
  - *Complete the transfer of FIMSA oversight from the Office of Management and Budget to DHS*
  - *Enhance collaboration between government and the private sector*

Cyber Ecosystem

- The cyber ecosystem envisioned at DHS is a system where we, in concert with our private and public partners, are able to prevent attacks rather than react to them.
- Three distinct building blocks are needed for the foundation of a healthy ecosystem:
  - *Automation* enables the ecosystem to continuously strengthen itself disorders by employing external defense systems
  - *Interoperability* enables seamless connections in places once blocked or gapped.
  - *Authentication* enables trusted online transactions and communications and helps protect personally identifiable information from hackers

National Strategy for Trusted Identities in Cyberspace

- Released by the Obama Administration in April 2011
- Seeks to resolve problems related to insecure passwords and user authentication
- Will create an Identify Ecosystem, in which there will be interoperable, secure and reliable credentials available to consumers who want them.

International Strategy for Cyberspace

- Released in May 2011, the foundation of the United States' international cyberspace policy is the belief that network technologies hold immense potential for our Nation and for the world.
- In July 2011 DHS signed a memorandum of understanding with India for cybersecurity for CERT to CERT cybersecurity collaboration.
- DHS works with its partners in the Federal Government, the State Department, the Department of Defense, and others, and the private sector to further the goal of an open and secure cyberspace.

Cybersecurity Awards Ceremony

- The Small Agency with the best overall security posture as indicated by the FISMA results was National Science Foundation (NSF):
    - Dan Hofherr, CISO
        - Andrea Norris, CIO

- The Large Agency with the best overall security posture as indicated by the FISMA results in Fiscal Year 2010 was Social Security Administration (SSA):
    - Brad Flick, CISO
    - Kelly Croft, CIO

Teri Takai

“The warfighter expects and deserves access to information – from any device, anywhere, anytime…”

DoD Information Enterprise Context

- Exploding technologies
- Demanding scope
- Increasing cyber threat
- Shrinking budgets
- Demanding efficiencies

DoD is transforming from “Stovepipes to Enterprise”

Salient Features of an Enterprise

Enough consistency and standardization to work together to…

- Increase information sharing efficiency
- Enhance mission effectiveness
- Improve information security
- Progress compatibility
- Boost collaboration

DoD Strategy for Operating in Cyberspace Five Pillars

- Cyberspace as a new operational domain
- New defense operating concepts
- Partner with Government and private sector
- Build relationships with our allies and partners
- Leverage the U.S.’ rapid technological innovation

Risk and Resilience

Challenge

- Reduce vulnerabilities and operate through a degraded environment

Approach

- Design-in at start; incorporate resilience in plans, operations, exercises and training

Emerging Technology

Challenge

- Reduce the time to leverage and securely incorporate new technology

Approach

- Stay ahead of the technology curve and share best practices

Collaboration Initiatives

Challenge

- Eliminate duplication, leverage technology, and share lessons learned

Approach

- Focus on whole-of-government needs and solutions

Policy and Management

Challenge

- Transform to information and knowledge- based enterprise

Approach

- Provide sufficient standardization to ensure access and sharing and leverage common opportunities

Matt Coose

Closing Ceremonies

- A sincere thank you to the conference planning and support team, the speakers, and attendees.
- We greatly appreciate your feedback on this event and specifically, around the future of the conference. We are looking at keeping it as is, combining with GFIRST, or simply not doing it altogether.
- As we all know, the hardest part of security is to driving action that reduces our risk.
- I ask that each of you take back what you discussed in the sessions and keynotes and try to convert some of this great info into action that actually improves our security posture and reduces risk at your agencies.