2013 Annual ACSC Conference Cyber Security Threat Sharing:

A Roadmap for Collaborative Defense

ACSC
Advanced Cyber Security Center

Bill Guenther

Charlie Benway

Ken Montgomery

Building Trust Between the Government and the Private Sector

One of the most critical ingredients to improving the nation's cyber security is increasing the trust between government agencies and the private sector, according to a U.S. cyber-security official.

"Response and mitigation can be done when you have knowledge, and knowledge happens when you have trust," said Phyllis Schneck, deputy under secretary for Cyber Security with the Department of Homeland Security's National Protection and Programs Directorate, during a presentation at the third annual ACSC conference.

In Schneck's view, the Department of Homeland Security should serve a central role in the process of sharing threat information and data between private companies and between those companies and the government. The department can serve as a type of "clearing house" that transcends competitive boundaries, she said.

Part of Schneck's role is to help government and industry become better collaborators and to put the processes in place such that it's commonplace for the public and the private sectors to work together.

Building the trust to make those relationships possible isn't always easy, said Schneck, who noted that the government hasn't always delivered a lot of great information to the private sector. It can also be difficult for companies, worried about their competitive positions, to share information outside the boundaries of their own organizations.

> **"Response and mitigation can be done when you have knowledge, and knowledge happens when you have trust."**
>
> *Dr. Phyllis Schneck, Deputy Under Secretary for Cyber Security, National Protection and Programs Directorate, Department of Homeland Security*

"I remember working a lot of attacks at my prior company where you had to choose between country and company. If you share the information out, was it going to cost us something? Was it going to drop stock prices the next morning?" said Schneck. "That should not happen."

According to Schneck, the goal is to develop "global situational awareness," in part by transforming networks into "ecosystems" that learn from every indicator that passes through it. By creating these mini-ecosystems, first, across multiple federal agencies, it will be possible to learn how they connect and how the data travels across the "weather map" of cyber attacks, said Schneck. By building partnerships with the private sector, additional data points can be added to the map.

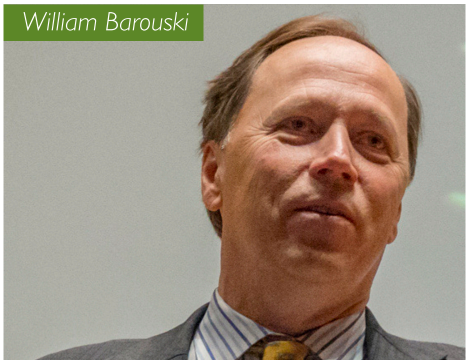
"We have the ability to defeat this lawless, well-funded adversary… by building trust and leveraging what we have together," said Schneck.

Dr. Phyllis Schneck

An Agenda for Automated Threat Sharing

The ACSC has achieved great results over its first two years and become a model for what a cross-sector, collaborative approach can produce. As the ACSC strives to quantify its progress in threat-sharing, there are four things to keep in mind according to William Barouski, executive vice president and chief information security officer, Federal Reserve System:

1. **Reach.** Currently, there are 28 members. There are 7,000 entities that participate in the Federal Reserve's electronic financial infrastructure. How do we leverage the power of the ACSC to extend its reach?
2. **Comprehension.** Organizations have different levels of cyber maturity, so it's important to keep in mind the varying levels of knowledge at different end points. Can an organization comprehend threat information and the implications of that information?
3. **Capability.** Comprehension is the first step. Then comes the ability to actually act upon the threat information in a way that enhances an organization's security. Some organizations will have that capability in-house. How do we help the other organizations, both to enhance their individual security and to protect the integrity of the broader system?
4. **Automated Threat-Sharing.** As cybersecurity continues to evolve, it needs to move beyond a process that relies on one-to-one communication toward a network of automated communication. Can we have an automated format, and what does it look like?


William Barouski

Mike Brown, Gary Gagnon, Denise Anderson, Kathleen Moriarty, Angela Gendron , Eric Burger

Advancing Federated Defense

Moderated by Mike Brown, this expert panel explored the opportunities and challenges in building a framework for federated cyber defense.

Mike Brown – It does come down to trust. We need to build our trust up, and while that may take federal legislation that creates the right environment for that trust to be developed, it will ultimately need to come from the private sector.

Gary Gagnon – One thing we could do more of is to take a step back and look at the trend lines of adversarial actions – what the adversary is doing and how they respond to our existing defenses – so we collectively as defenders can institute new ways to try and stop attacks.

Denise Anderson – Having clear guidelines for what type of information should be shared and when – such as the ISAC's Traffic Light protocol, which aligns indicators to a red, amber, green or white level – can help increase the level of threat-sharing.

Kathleen Moriarty – It's great to share within groups like the ACSC, but we should consider how we can have a bigger impact. The current approach leaves small and medium-sized organizations vulnerable, which matters because they are part of the larger supply chain.

Eric Burger – There are a number of barriers to threat-sharing, including legal questions, liability issues, and differences between countries in what can or can't be shared. The question we need to answer is: What can we do and what incentives can we put in place that will make enterprises want to share?

Angela Gendron – The more an organization shares, the more vulnerable it makes itself. Threat-sharing is a positive development, but we do need to understand there is a potential downside, and we need to manage that as well.

Afternoon Break-Out Sessions

Wirespeed Threat-Based Defense

There is no hard-and-fast definition for wirespeed, but generally, it stands for being able to transact data at the speed at which it's actually happening in a company's environment: take the meta-data as it's happening, share it and then act on it. Today, cyber security is largely reactive, but the eventual goal is to transform into a more proactive, or preventative, system where the sharing of threat indicators in real (or near-real) time can prevent attacks. To do this, there will need to be a shift in the balance between what is automated and what is done by people.

- The ultimate goal is to spend less time doing the "boots on the ground" sharing and more time taking what we've learned from the sharing and **applying it to our own environments.**
- Instead of attempting to protect everything, we need to work on identifying what's really important, communicating that broadly, and then **building internal mechanisms to automate** the protection of the right things at the right time.
- While there are a lot of aspects to threat-sharing and a threat-based defense that can be automated, **the human element will never be entirely removed.**
- We need to first decide what success looks like when it comes to cyber security and a wirespeed threat-based defense and then **develop a vision** or plan for how to achieve that success.

Security, Outsourcing and the Cloud

As organizations of all sizes are facing an unprecedented increase in the number of cyber threats and grappling with a legacy of vulnerabilities, they are trying to determine how to be ready to rapidly respond to these threats in order to best protect themselves. Not all organizations have the internal capacity to mitigate risk and deal with threats. One option on the table is to leverage outsourcing options for cyber security, which poses its own set of questions: What might companies outsource, and how do they make that decision?

- When companies turn to outsourcing, it's important they understand their internal capabilities and their culture, so they can **manage the roll-out** instead of just letting it happen.
- Companies can outsource functions, but they **can't outsource risk**: companies remain accountable for what happens with their system and their data.
- The move to the cloud is happening, so companies shouldn't fight it but should instead **focus on leveraging the evolution of the cloud** in ways that can help them.
- When outsourcing, companies should follow tight discipline in understanding the business case, structuring the contract, building in SLAs and **continuing to measure and assess.**

Executive Order Implementation and Related Policy Issues

Organizations large and small have been reacting to the President's sharp focus on cyber security and seeking guidance on how to comply. As a result of the lack of legislative action, the Executive Order (EO) 13636, "Improving Critical Infrastructure Cybersecurity," and Presidential Policy Directive (PPD) 21, "Critical Infrastructure Security and Resilience" were issued this year. While voluntary information sharing, building frameworks, and public-private partnerships are moving the discussion forward, challenges remain for more swift implementation.

- A threat sharing goal is to **make it easier for the government to share unclassified information**, with an emphasis on indicators and not necessarily threat content.
- **Regionalization** has come to the forefront in discussions as a means to better track threat sharing systems.
- It is important to strike a balance between the instinct to readily share information for managing risk with the **liability issues** on the back end.
- Technology is the best way to protect information using a **data-centric approach**. Encryption, for example, can provide one of the best solutions.
- In Research and Development, **partnerships play a significant role** in how solutions are transformed into practical applications.

James Caulfield, Paul Morville, Tom Mahlik, and David Williams leading the "Wirespeed Threat-based Defense" panel.

National Cyber Policy Outlook

As the number of cyber attacks has skyrocketed in recent years, the threat of those attacks and the potential damage they can inflict have consequences for the nation's economy of a magnitude this country has never seen before, Rep. William Keating said during a keynote address at the annual ACSC conference.

> **"One attack successfully made could shut down the entire Eastern Seaboard of the United States."**
>
> *Congressman William R. Keating, United States House of Representatives; Cybersecurity, Infrastructure Protection and Security Technologies Subcommittee Member, House Committee on Homeland Security*

No company or industry is immune from the threat of cyber attacks, which is why the bottom-up, cross-sector approach employed by the ACSC is effective in pursuing creative solutions that overcome some of the bureaucratic obstacles endemic to this issue, according to Keating.

Keating said he realized that Congress does not have deep technical expertise on cyber security. However, it has to be part of the dialogue in developing solutions as Congress will play a critical role in developing an overall policy and legislative framework to guide the country's efforts, according to Keating.

U.S. Congressman William Keating

Highlights from Keating's remarks:

- There is a need for regulatory standardization on cyber security issues across international borders: it will be difficult, but it could also present significant economic benefits.
- However, a top-down regulatory approach is not the right answer as it will not be able to keep pace, or be flexible enough, to deal with the rapidly evolving threats.
- Small and medium-sized businesses need to be incorporated into the solution, as these companies may not have the resources needed to keep pace with the requirements for preparing, mitigating and preventing cyber attacks.

Participants included in the ACSC Annual Conference:

Special Thank You to Conference Sponsors: **.406 Ventures** and **Allied Minds**

Denise Anderson, Vice President, Government and Cross-Sector Programs, Financial Services Information Sharing and Analysis Center (FS-ISAC)

William Barouski, Chief Information Security Officer, Federal Reserve System

Charlie Benway, Executive Director, ACSC

Mel Bernstein, Senior Vice Provost for Research and Graduate Education, Northeastern University

Mike Brown, Rear Admiral, USN (Ret), VP and General Manager, RSA Global Public Sector

Eric Burger, Research Professor of Computer Science and Director, Georgetown Center for Secure Communications, Georgetown University

James Caulfield, Program Manager, Advanced Threat Protection, Federal Reserve National IT Services

Oswin Deally, Senior Director for Enterprise Information Security Operations, Liberty Mutual

Greg Dracon, Principal, .406 Ventures

Demetrios Eleftheriou, Senior Counsel, Privacy and Data Security, EMC Corporation

William Fandrich, Senior Vice President and Chief Information Officer, Blue Cross Blue Shield of MA

Matthew H. Fleming, Fellow, Homeland Security Studies and Analysis Institute

Gary Gagnon, Senior Vice President and Chief Security Officer, The MITRE Corporation

Angela Gendron, Senior Fellow, Canadian Centre of Intelligence and Security Studies, Carleton U.

William Guenther, Chairman and Founder, ACSC

Congressman William R. Keating, U.S. House of Representatives

Robert Kolasky, Director of the Integrated Task Force, U.S. Department of Homeland Security

Tom Mahlik, Deputy Chief Security Officer and Director, Global Security Operations, The MITRE Corporation

John McKenna, VP and Chief Information Security Officer, Liberty Mutual Group

Kenneth Montgomery, First Vice President and Chief Operating Officer, Federal Reserve Bank of Boston

Kathleen Moriarty, Global Lead Security Architect, EMC Corporation

Mark Morrison, Senior Vice President and Chief Information Security Officer, State Street Corp.

Paul Morville, Vice President of Products and Co-Founder, Confer

Phyllis Schneck, Deputy Under Secretary, Cyber Security, National Protection and Programs Directorate, U.S. Department of Homeland Security

John Schramm, Vice President, Global IS Risk Management Division & Chief Information Security Officer, Manulife Financial

Howard Shrobe, Associate Director & Principal Research Scientist, MIT Computer Science and Artificial Intelligence Laboratory

Scott Tousley, Deputy Director, Cyber Security Division, Science & Technology Directorate, U.S. Department of Homeland Security

Michele Whitham, Partner, Foley Hoag LLP

David R. Williams, CISSP, Threat Intelligence and Incident Response, Pfizer