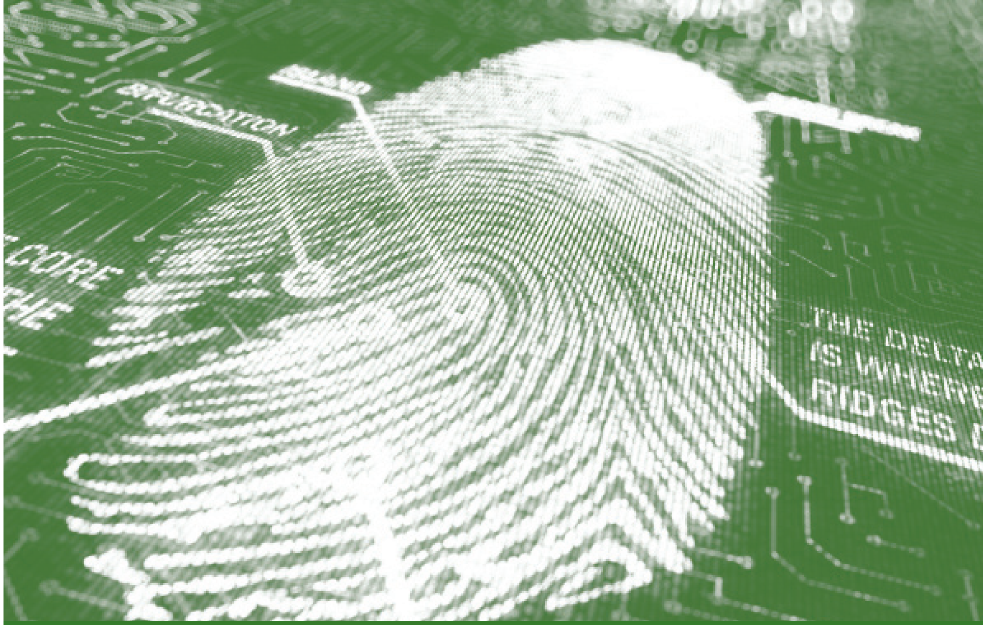

ACSC

Advanced Cyber Security Center

“Organizing Public-Private Assets to Solve Grand Challenges”

2012 Annual New England Conference Summary Report

Cyber Security Grand Challenges:

Securing data sharing between industry and university researchers
Despite interest from both sides in expanded data sharing, significant technological and legal obstacles exist. How can information be encrypted and anonymized so that researchers are able to leverage large data sets from industry in a secure manner?

Developing next-generation resilient systems
“Built-in security” must replace harmful ad-hoc patch mentality in order to move us towards the next generation of resilient systems. Faced with the reality that the enemy is often already “inside,” machines must be designed with the capability to segment and protect the highest-value data.

Implementing standards for software and systems
Development of voluntary minimum best practice operating standards for users and technology developers. Agreement on more controversial establishment of legal standards and liabilities for basic security.

Facilitating collaborative real-time defenses and forensics
New collaboration strategies are needed to build situational awareness, keep pace with attackers and respond to increasingly sophisticated threats. Real-time, automated sharing is necessary to develop predictive analytics and move industry beyond post-facto forensics.

Defining limits of cyberwarfare behavior and automation rules
What constitutes an act of war in the digital domain? In managing the oversight process, how are human judgements coordinated and controlled in an automated environment where machines react to each other in a microsecond?

Cloud security transparency
Growth of the cloud ushers in new dangers, including more concentrated attack targets, single point of failures, and malicious co-tenants. Lack of visibility impedes ability to verify security assessments.

ACSC: Launched and supported by:

Mass Insight
GLOBAL PARTNERSHIPS

ACSC

On November 15, 2012, The Advanced Cyber Security Center, supported by Mass Insight Global Partnerships, convened the "Second Annual New England Conference: Organizing Public-Private Assets to Solve Grand Challenges."

ACSC ROLE:

To bundle and broker multi-university academic collaborations with industry partners to respond to large scale, multi-disciplinary cybersecurity challenges that are common priorities for the federal government and industry.

CONFERENCE GOALS:

To identify $10 million+ R&D challenges and the organizing steps, incentives and policies that are required for a collaborative nonprofit like the ACSC to organize research partners in the region.

ACSC Members:

Biotech/Pharmaceuticals
Biogen Idec
Boston Scientific Corporation
Pfizer Inc.

Defense
Draper Laboratory
MIT Lincoln Laboratory
The MITRE Corporation

Financial Services
Eastern Bank
Federal Reserve Bank of Boston
Fidelity Investments
John Hancock Financial Services
Liberty Mutual Group
State Street Corporation

Government
Commonwealth of Massachusetts

Health Care
Blue Cross Blue Shield of MA
Harvard Pilgrim Health Care
Partners HealthCare System Inc.

Legal
Foley Hoag

Technology
Akamai
Bit9
RSA/EMC Corporation
Veracode

University Consortium
Boston University
Harvard University
MIT
Northeastern University
University of Massachusetts
Worcester Polytechnic Institute

“*The intersection of policy, law, social science, and technology is what makes this region extraordinary in terms of having the assets to deal with the cyber security challenge.*”

William Guenther
Mass Insight Global Partnerships

“*We pride ourselves on addressing society's "grand challenges." We're not only creating an economic opportunity, we're addressing a social issue of importance to the country and the world. That's our tradition in New England.*”

Massachusetts Secretary
Gregory Bialecki

“*There would be a different data interaction if we focused on sharing as opposed to transacting. If academics could get access to industry's real data, we could do more relevant research than we can do with the generated data we have now.*”

Dr. James Waldo
Harvard University

“*We also have to build our systems to be resilient to human behavior – to understand how people interact with the internet and then create policies, procedures, and laws to keep systems secure.*”

Dr. Jack Wilson
University of Massachsuetts

“*Large software companies create critical infrastructure by deploying their products on virtually every laptop with no requirements in regards to cybersecurity. It's astonishing.*”

Maria Cirino
.406 Ventures

“*We've moved to an era where intelligence-based security is not an option any longer - it's a necessity. Advanced threats require faster detection and faster response to win the race against time.*”

Tom Heiser
RSA, The Security Division of EMC

“*You've got to work at this public-private partnership and you need to be agile; not just in cyber defense but in the way you think about the organization and take the opportunities as they come.*”

Dr. Steven King
U.S. Department of Defense

“*Perhaps the biggest negative is the lack of auditor and tenant visibility that occurs when resources are migrated into the cloud. This lack of visibility is a deficiency in this emerging critical infrastructure that the cloud represents.*”

Dr. Ari Juels
RSA and RSA Laboratories

“*There's no certainty yet on which training opportunities lead to a stronger individual or a stronger team. Figuring out how to create an outcome-based approach to cyber security education is something worth thinking about.*”

Scott Tousley
U.S. Department of Homeland Security

ACSC Work Groups: Ongoing and Potential Initiatives

Areas of Focus	*Identified Challenges*	*Recommendations*
Big Data, the Cloud, and Next Generation Secure Computing *The ACSC’s R&D Prime the Pump project titled, “A Platform for Data-Intensive Cybersecurity Monitoring” has been working on preparing event stream industry data for real-time analysis along with data protection and has been integrated into the ACSC NSF grant proposal for Secure and Trustworthy Cyberspace.*	• Most security with big data is reactionary and occurs forensically with historical data. • Difficult for researchers and academics to get data, feeds, and systems from industry to test theories and pilot next generation solutions. • Industry, taxed by their operations, does not have the bandwidth to devote time to collaborate with researchers or implement large-scale solutions. • Without a barrier to cloud entry, agreed-upon standards are difficult to enforce.	• Create a better data summarization process and implement a real-time detection system and real-time counter attack. Seek on-demand elastic computing. • Develop a sandbox concept with real systems and anonymized data to put theory to practice. • Seek incremental new solutions where IT staff can manage transitions and proper implementation. • Communicate policies and procedures for entering big data in the cloud.
Maximizing Cybersecurity Investments: Risk Analysis, Metrics, and Incentives for Better Defense *The ACSC’s R&D Prime the Pump project titled, “Cybersecurity Risk Analysis and Investment Optimization” has been developing models for cyber risk and the costs and benefits of various technologies along with techniques for integrating these models as part of a holistic risk management strategy; this project was also part of the ACSC NSF grant proposal for Secure and Trustworthy Cyberspace.*	• Problems, compromises, and security issues are often identified after they occur. • The scope of cyber security issues appears undefined and too broad for VCs to identify viable investments. • The privacy layer between the federal government and industry prevents the commercialization of technologies transferable to the private sector.	• Focus on developing prolific solutions that are preventative and based on lessons learned. • Technologists and financial experts need to collaborate to present cogent business cases for funding. • Encourage public-private partnerships to develop government solutions for industry use.
Threat Sharing: The New Discipline of Cybersecurity *The ACSC established a bold vision for a cross-sector, in-person threat sharing model built on trust among a manageable-sized group of security practitioners brought together through regular bi-weekly meetings. The ACSC is growing to build a more universal and secure threat sharing network.*	• Identifying the expanding source of threat agents requires a reach beyond the 27 member group. • Policy issues are often masqueraded as legal issues which prohibits investigation. • Existing and assumed legal barriers hinder meaningful, automated threat sharing.	• Set standards to aggregate expanded data and use the actionable information in an intelligence-driven security model. • Pursue policy that promotes shared information when risk to others is identified. • Explore and research laws/amendments to fully comprehend restrictions and/or opportunities.

Speakers in the ACSC Second Annual New England Conference: "Organizing Public-Private Assets to Solve Grand Challenges"

ACSC

Government

Gregory Bialecki
Secretary, MA Executive Office of Housing and Economic Development

Timothy Edgar
Senior Legal Advisor, Office of the Director of National Intelligence

Dr. Steven King
Deputy Director for Cyber Security in the Information Systems and Cyber Security Directorate of ASD (R&E). U.S. Department of Defense

Dr. Herbert Lin
Chief Scientist, Computer Science & Telecommunications Board, National Research Council of the National Academies

William Newhouse
Cybersecurity Program Lead, National Institute of Standards and Technology

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

Industry

Dr. Robert Brammer
President and CEO, Brammer Technology

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

Maria Cirino
Co-Founder and Managing Director, .406 Ventures

Christopher Harrington
Consulting Security Engineer, RSA, The Security Division of EMC

Tom Heiser
President, RSA, The Security Division of EMC

Dr. Ari Juels
Chief Scientist, RSA, The Security Division of EMC and Director, RSA Laboratories

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

Christopher Perretta
Chief Information Officer, State Street Corporation

Alexander Popowycz
Vice President, Enterprise Information Security, Fidelity Investments

Thomas Quinn
Chief Information Security Officer, BNY Mellon

Matthew Richard
Principal InfoSec Engineer, The MITRE Corporation

Bob Rudis
Director, Enterprise Information Security and IT Risk, Liberty Mutual Group

David Saul
Senior Vice President and Chief Scientist, State Street Corporation

Dr. Nikos Triandopoulos
Principal Research Scientist, RSA Laboratories

David Williams
Threat Intelligence and Incident Response, Pfizer

University

Dr. Azer Bestavros
Professor, Computer Science Department and Director, The Hariri Institute for Computing, Boston University

Dr. Wayne Burleson
Professor of Electrical and Computer Engineering, University of Massachusetts Amherst

Dr. Stephen Chong
Assistant Professor of Computer Science, School of Engineering and Applied Sciences, Harvard University

Dr. George Cybenko
Dorothy and Walter Graham Professor of Engineering, Thayer School of Engineering, Dartmouth College

Dr. Srini Devadas
Edwin Sibley Webster Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology

Dr. David Luzzi
Executive Director, Strategic Security Initiative, Northeastern University

Dr. John Savage
An Wang Professor, Department of Computer Science, Brown University

Dr. Evimaria Terzi
Assistant Professor, The Hariri Institute for Computing and Junior Faculty Fellow, Computer Science Department, Boston University

Dr. James Waldo
Gordon McKay Professor of the Practice of Computer Science and Chief Technology Officer, Harvard University

Dr. Jack Wilson
President Emeritus, University of Massachusetts and Distinguished Professor of Higher Education, Emerging Technologies, and Innovation, University of Massachusetts Lowell

Mass Insight
GLOBAL PARTNERSHIPS

Mass Insight Global Partnerships, founded in 1989, is a Boston-based consulting and research firm that builds strategic pre-competitive alliances between higher education, industry and government, both regionally and globally. Mass Insight organizes collaborative, performance-based leadership initiatives supported by individual members, and uses communications, publications, policy research and public opinion surveys to shape public-private actions and develop innovative partnerships. The Advanced Cyber Security Center was launched and is supported by Mass Insight Global Partnerships.

18 Tremont Street, Suite 1010, Boston, Massachusetts 02108 • 617-778-1500 • www.massinsight.com

The Advanced Cyber Security Center (ACSC) is a nonprofit corporation supported by Mass Insight Global Partnerships that brings together industry, university, and government organizations to address sophisticated advanced cyber security challenges.

Focusing on cross-sector collaboration, the ACSC develops unique approaches to share cyber threat information, to engage in next-generation cyber security research and development, and to create education programs to develop cyber security talent.