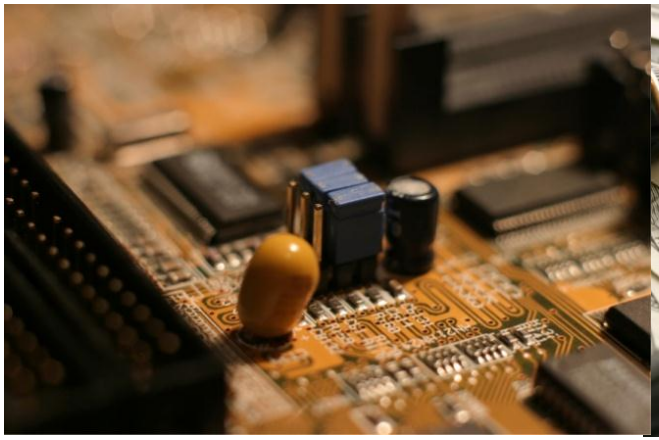


ADVANCED CYBER SECURITY CENTER

Bill Guenther, Chairman, CEO and Founder
Mass Insight Global Partnerships

Robert F. Brammer, Ph.D., President and CEO
Brammer Technology, LLC

CSF Conference
June 25, 2012

An Initiative of
Mass Insight
GLOBAL PARTNERSHIPS

18 Tremont Street, Suite 930
Boston, MA 02108
www.massinsight.com

The New England Goal

"The **New England region** is committed to be **a global leader** in confronting current and future cyber security challenges and to reinvigorate Route 128 to be the '**national cyber security beltway**.'"

From the White Paper Executive Summary
produced on behalf of the ACSC
and the five university members of the
Massachusetts Green High Performance Computing Center
(Boston University, Harvard, MIT, Northeastern, UMass)

New England Cyber Security:

The Benchmarks

First Adopter for Leading Edge Security Practices and Technology: Industry, Universities, Government

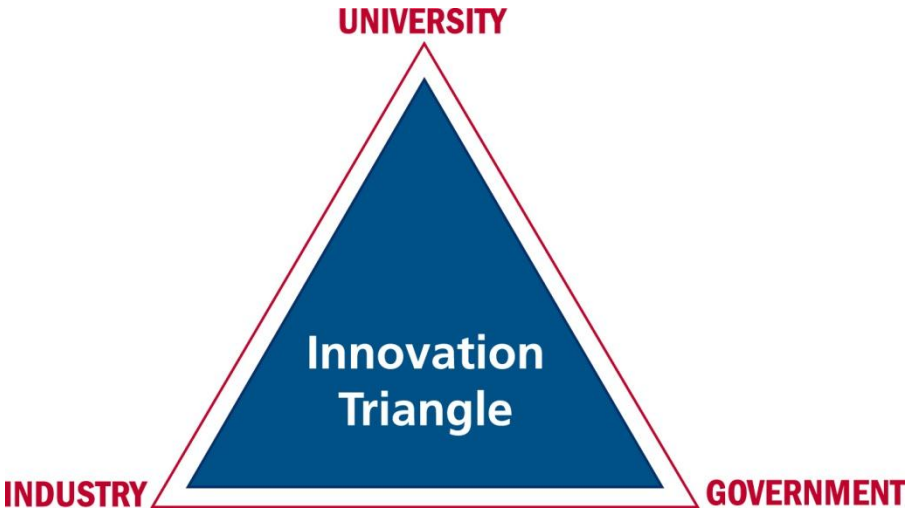
National/Global Player in R+D and Education

- The leading **university research** center
- A major corporate IT/cyber security **R+D and industry location**
- The **#1 choice** for students based on academic programs and industry internships/work-study

Flagship R&D Centers: A Pre-Competitive Paradigm
Industry-University-Government Partnerships

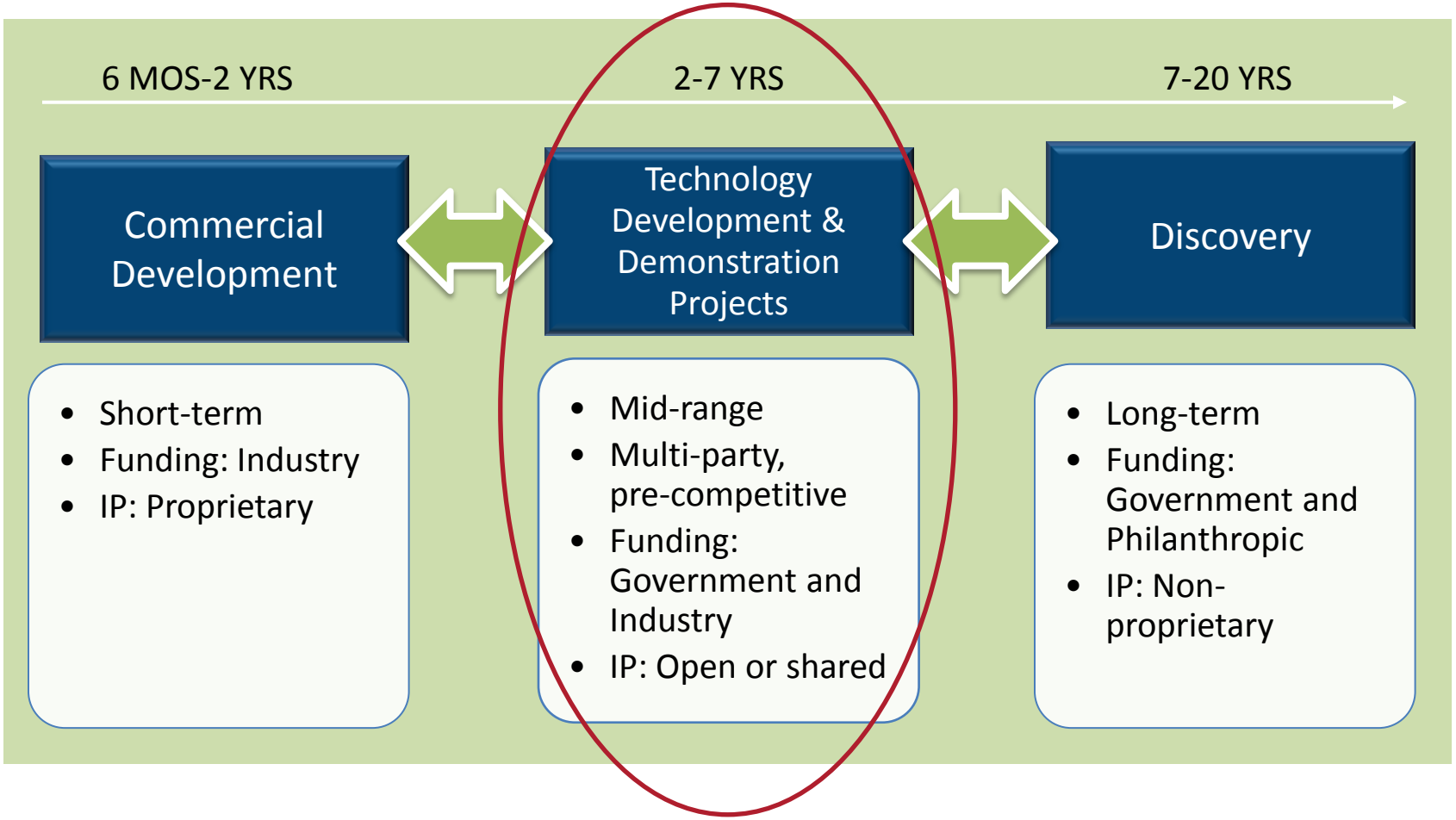
Networking, bundling, brokering talent and ideas.

"Bridging" space for the three partners.



Industry-University-Government Partnerships

The Innovation Timeline



The Advanced Cyber Security Center

The Advanced Cyber Security Center is a **cross-sector collaboration** organized to help protect the region's organizations from the rapidly evolving advanced and persistent cyber threats…

……and to **support New England's role as a center for cyber security R+D, education, talent and jobs.**

ACSC Charter Members and Partners

(as of June 2012)

Defense
Draper Laboratory
MIT Lincoln Laboratory
The MITRE Corporation

Government
Commonwealth of Massachusetts

Legal
Foley Hoag

Technology
Akamai
RSA/EMC Corporation
Veracode

Bio/Pharma
Pfizer
Boston Scientific

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

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

MGHPCC University Consortium
Boston University
Harvard University
MIT
Northeastern University
University of Massachusetts

Other Academic Partners:

- Babson College
- Brandeis University
- Brown University
- Middlesex Community College
- Tufts University
- Worcester Polytechnic Institute

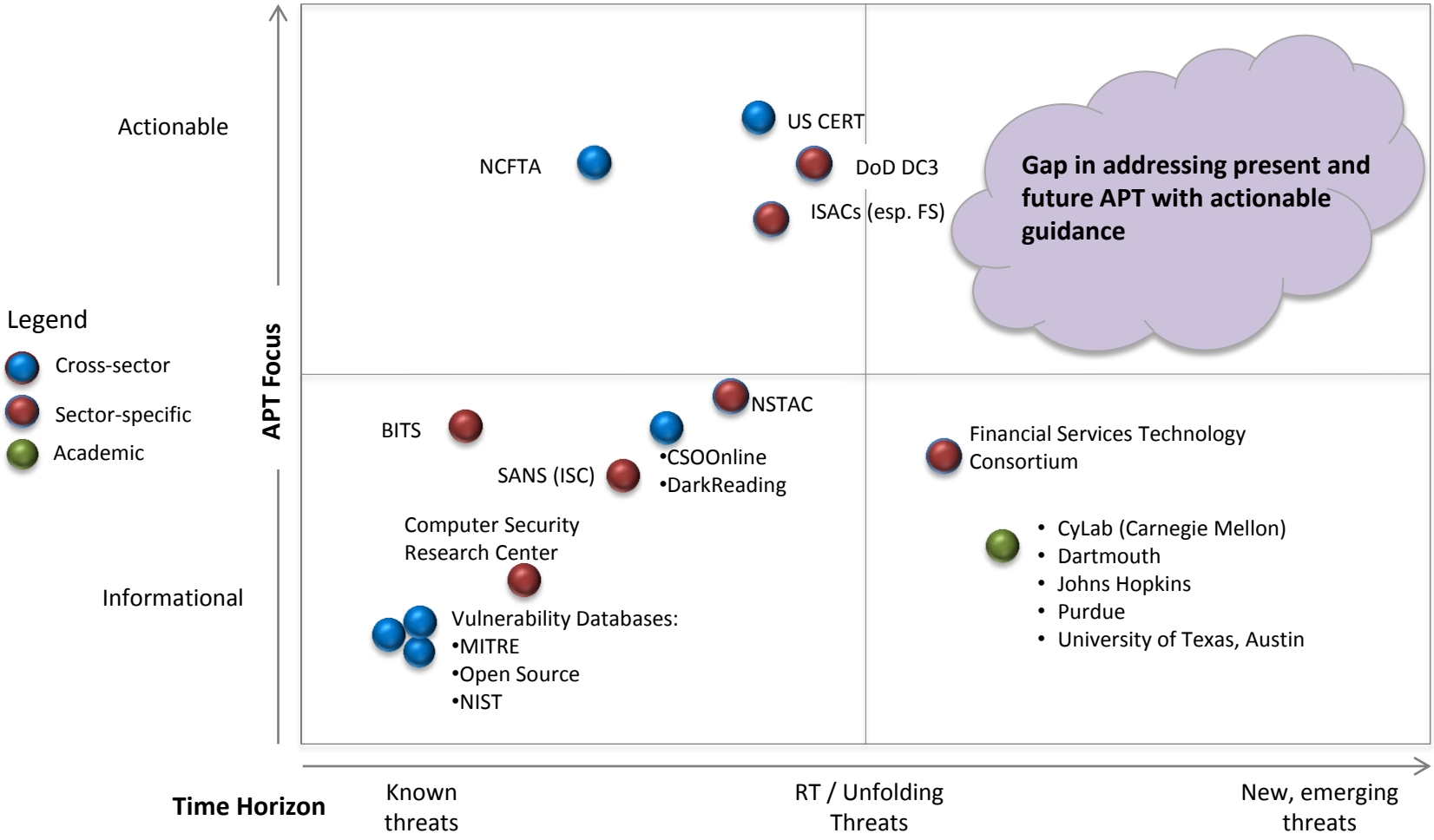
Advanced cyber threats: Collaboration is key - no single organization can respond effectively

		Interviews with ACSC Members
Attacks are increasingly sophisticated	• The APT* will customize their malware to target each specific organization…Malware is continually updated to ensure that it cannot be easily detected…(Mandiant 2010) • 56% of breaches require months to years to contain. (Verizon 2010 Data Breach Report)	*"Unlike most firms, we're configured so we can see where traffic is coming from and* ***we're seeing a lot more attacks in the last six months*** *that look like they're coming from state-sponsors."* *"We watch these attackers and we know them. Some are very fast moving…If you lose track of them in your system* ***you can lose them for months, if not forever****."*
Current solutions are not adequate	• 16% of breaches are discovered via active, deliberate detection. (Verizon) • Only 24% of APT malware is detected by an anti-virus solution. (Mandiant 2010)	*"There are plenty of security solutions available. The problem is that they all focus on one thing. To deal with today's attackers, It's* ***imperative to look across the stack & connect the dots…*** *This is hard. We need to figure out how to do it."* *"****We are not keeping pace*** *with attacker innovations."*
Organizations want to increase the sophistication of their employees & solutions	• …the value of monitoring (perhaps we should say "mining") logs cannot be overstated. The signs are there; we just need to get better at recognizing them. (Verizon 2010 Data Breach Report)	*"We contract out & have a pretty rich array of security services. What* ***we need is to cultivate the investigative mindset*** *of our staff. That will be key to improving our ability to detect and block."* *"We are in reactive mode.* ***We need to think much more creatively and develop proactive approaches…*** *Breaches are not acceptable. We need to anticipate the attacker and there's no reason why we can't."*

Mass Insight GLOBAL PARTNERSHIPS

"APT": Advanced Persistent Threat is the label applied to the most serious and complex cyber attackers. They are professionals and may be state-sponsored.

A New Hybrid Paradigm:
ACSC and Existing Collaborations



The Advanced Cyber Security Center

The Advanced Cyber Security Center is a **cross-sector collaboration** organized to help protect the region's organizations from the rapidly evolving advanced and persistent cyber threats…

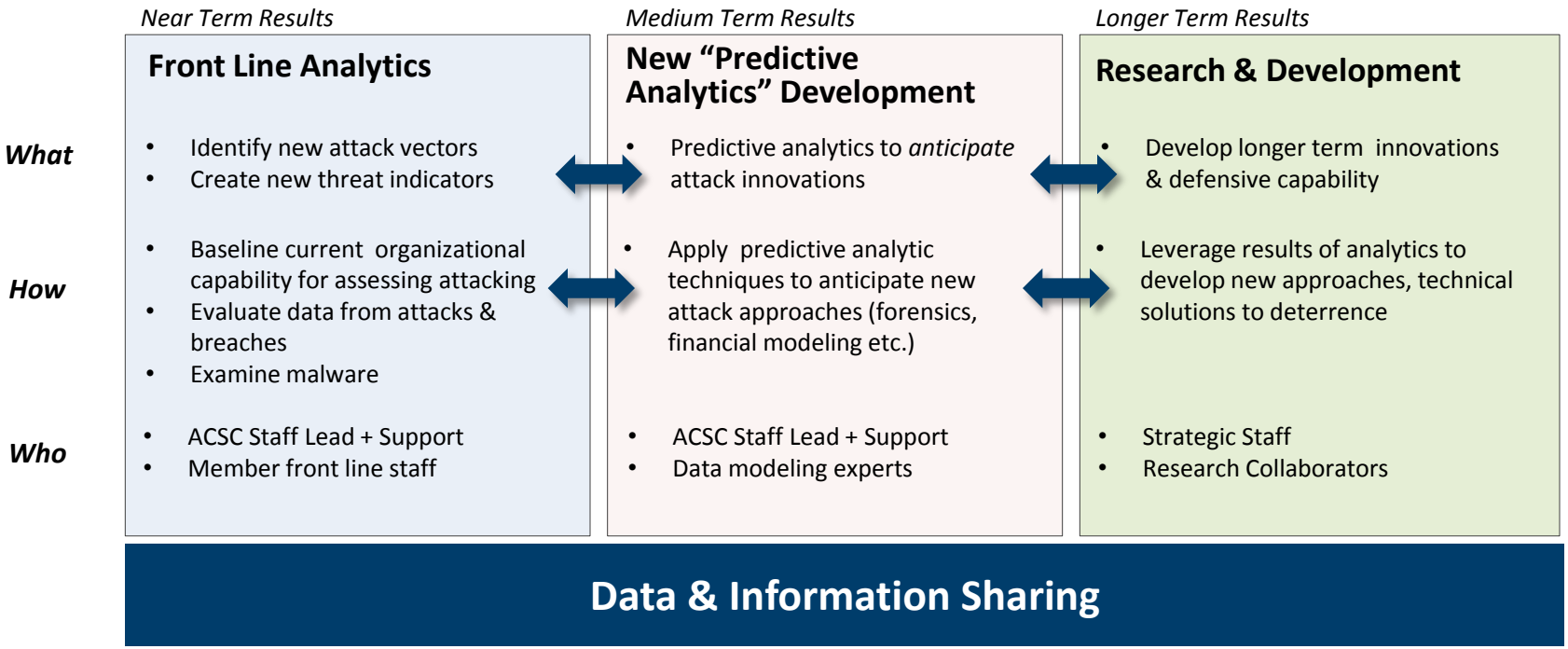
……and to **support New England's role as a center for cyber security R+D, education, talent and jobs**.

Three Key Initiatives:

Information Sharing	R&D and Education	Policy Development
• Identify new threat indicators • Share Best Practices • Build X-industry network in NE	• Development of Cyber Workforce • Address hardest R&D challenges • Government, Industry & Higher Ed Funded	• ACSC as best practice laboratory • Research on information sharing, • Federal legislation

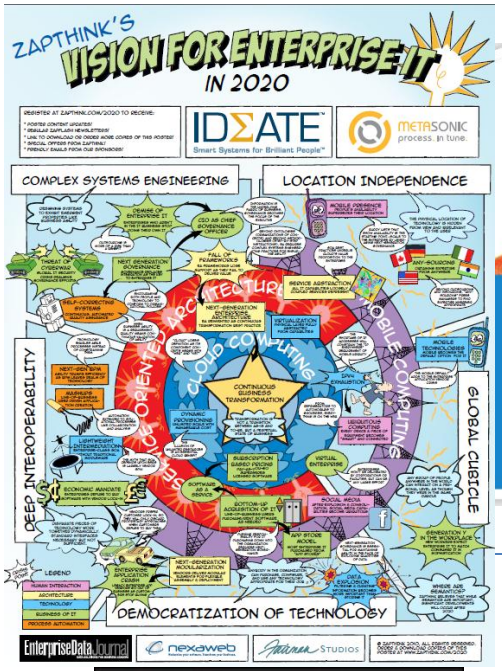
ACSC:
Strengthening short term defenses & longer term capability

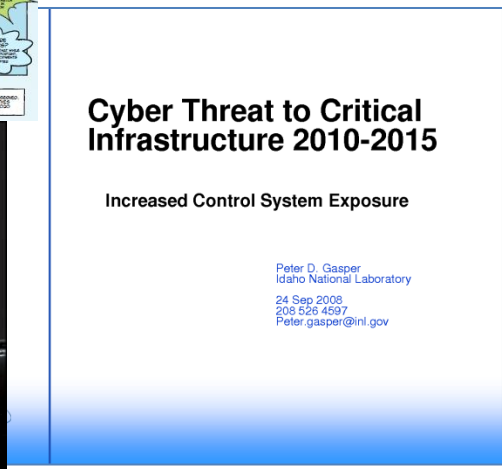
- The ACSC will deliver actionable intelligence to bolster an organization's defenses in the short term and generate new defensive strategies and R+D in the longer term.



Enterprise Systems, Critical Infrastructure, and Cyber Threats in 2020 – Implications for Security Management

- Enterprises
  - Increased agility due to collaboration, mobility, virtualization, cloud-based operations, real-time predictive analytics
- Critical Infrastructure
  - Increased integration with IT and networks
  - Cost, environmental, security pressures
- Cyber threats
  - Increasing sophistication and targeting with more investment by nation states and NGO's
  - Growth of cyber offense economy
- Implications for Security Management
  - Integration with enterprise management
  - Prevention remains important, but more needs for real-time and predictive response
  - Revised workforce and automation strategy



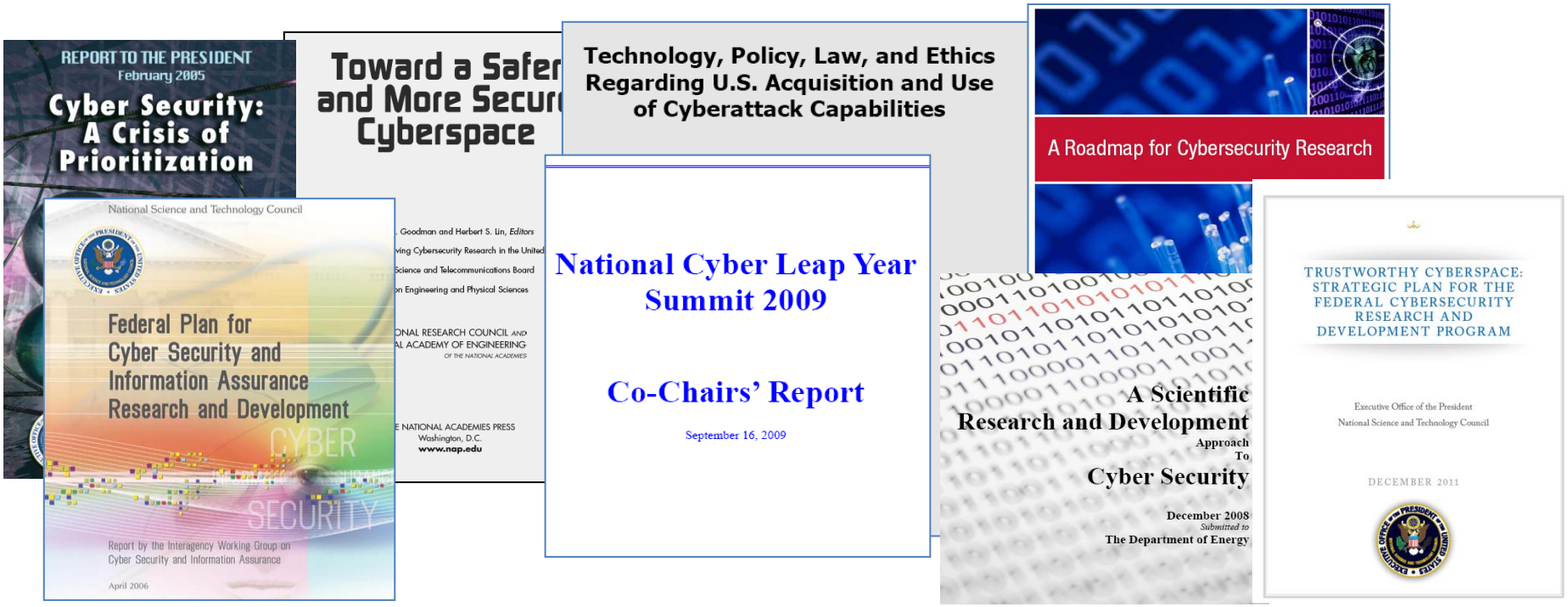


Cyber Security Research Agenda

- **Foundations for Cybersecurity (13 subtopics)** – e.g., secure hardware, firmware, and software engineering, cryptology, multi-level-security and cross-domain solutions, cyberspace situational awareness, access, anonymity, privacy, …
- **Cybersecurity and Information Assurance Characterization and Assessment (11 subtopics) --** e.g., certification and accreditation, quality assessment, security metrics, …
- **Cybersecurity for Internet and Control System Infrastructure (6 subtopics)** -- e.g., secure networking protocols, telecom and SCADA security, …
- **Functional Cybersecurity (9 subtopics)** – supply chain management, ID management, SOC management, forensics, …

- **Domain-Specific Cybersecurity (12 subtopics)** – e.g., infrastructure dependencies, tactical/airborne military networks, banking and finance systems, power grid, health IT systems, …
- **Cyberattack and Cyberexploitation (5 subtopics)** -- e.g., technology and operational issues, …
- **Next-Generation Systems and Architectures (9 subtopics)** -- e.g., moving target architectures, tagged architectures, converged network, storage, and server protocols and operations, homomorphic encryption, secure green IT, autonomous adaptive systems, quantum computing and cryptography, …
- **Social Dimensions of Cybersecurity (8 subtopics) –** e.g., cybersecurity economics, Internet ethics and trust, international law and policies, military information operations, useable security, privacy legislation and regulation, …

We Review Federal Cybersecurity Research Plans and Programs as Inputs to our Strategy



- Requirements for cybersecurity research have been assessed many times by organizations like the National Academies, the National Science and Technology Council, the Federal Networking and Information Technology R&D Program, OSTP, DOD, DOE, DHS, and others
- Some 2012 federal budget items -- DOD cybersecurity R&D - $2.3B, NSF Secure and Trustworthy Cyberspace - $112M, NIST Secure and Robust Cyber Infrastructure - $43M, …

TRUSTWORTHY CYBERSPACE: STRATEGIC PLAN FOR THE FEDERAL CYBERSECURITY RESEARCH AND DEVELOPMENT PROGRAM

December 2011

Strategic Thrusts

- **Inducing Change** –game-changing themes to direct efforts towards disrupting the status quo to improve the security of the critical cyber systems and infrastructure that serve society.

- **Developing Scientific Foundations** – Developing an organized, cohesive scientific foundation to the body of knowledge that informs the field of cybersecurity

- **Maximizing Research Impac**t – Catalyzing integration across the game-changing R&D themes, cooperation between government and private-sector, strengthen linkages to other national priorities, e.g. health IT and SmartGrid.

- **Accelerating Transition to Practice** – Focusing efforts to ensure adoption and implementation of the powerful new technologies and strategies that emerge from the research themes, and the activities to build a scientific foundation so as to create measurable improvements in the cybersecurity landscape.

Game-Changing R&D Themes

- **Designed-In Security** – Builds capabilities to develop, and evolve high-assurance, software-intensive systems . Enable simultaneous development of cyber-secure systems and associated assurance evidence

- **Tailored Trustworthy Spaces** – Provides flexible, adaptive, distributed trust environments to support functional and policy requirements arising from a wide spectrum of activities and evolving threats.

- **Moving Target** – Create, analyze, evaluate, and deploy mechanisms and strategies that continually change to increase complexity and cost for attackers and limit attack opportunities.

- **Cyber Economic Incentives** – Develop effective incentives to make cybersecurity ubiquitous. Incentives may involve market-based, legal, regulatory, or institutional interventions and must be based on sound metrics and sensible notions of liability and care. Requires advances in understanding both markets and humans, and interactions with technical systems.

New England Cybersecurity Research Strengths
(Based on a Study by ACSC Member University Faculty*)

- **Trusted Interactions in Cyberspace** -- technologies for trusted identities, digital rights management and enforcement, cyber law enforcement, privacy-enhancing regulations and technologies, …

- **Certifiable Software and Systems** -- safe programming languages, formal verification and automated theorem proving, composable formal security analysis, secure embedded software and systems, …

- **Cyber Situational Awareness** -- economics models for risk assessment and management, game-theoretic adversarial/threat modeling, federated, cross-organizational monitoring, real-time big data analytics, …

- **Secure Outsourcing of Data and Computation** -- expressive security SLAs, computing over encrypted data, homomorphic encryption, differential privacy, data integrity in the cloud, access control and policy deconfliction, …

* Study team led by Azer Bestavros, Boston U.; Wayne Burleson, UMass Amherst, Frans Kaashoek, MIT; Greg Morrisett, Harvard

Areas for Possible ACSC-funded Research Projects*

1. Integration of Cyber Security Risk Frameworks with Enterprise Risk Frameworks
   - Need for common view of risks affecting the enterprise. Important for resource allocation.

2. "Big Data" Management for Cyber Security Operations
   - Current cyber security tools do not scale well to the enterprise level for our major partners. Need scalable systems to enable real-time analysis and decisions to address advanced cyber threats.

3. Automation Processes and Technology for Cyber Security Information Sharing
   - Efficient sharing of security information requires standardization and technology to promote collaborative analysis and actions.

4. Security and Privacy for Mobile Devices
   - BYOD challenges. Need high levels of security and privacy for these devices.

5. Optimization of Enterprise Security Architectures
   - How can a security architecture be optimized to get the most value from the security budget?

*Based on member interviews.

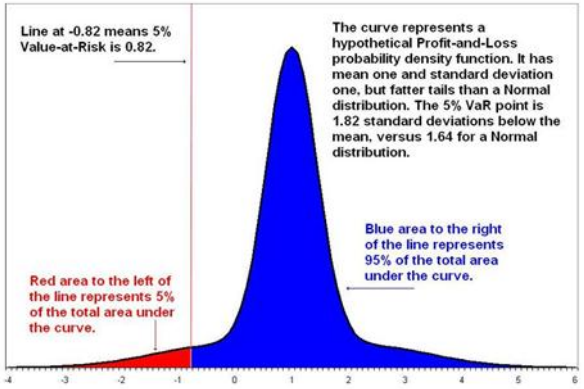
ACSC Research Project #1
Cybersecurity Risk Analysis and Investment Optimization

- Multi-disciplinary, multi-institutional project funded by our financial services industry members – Fidelity, John Hancock, Liberty Mutual, State Street

- UMass PI's from CS, Finance, Operations Management, and IT Security

- The vision of this project is eventually to have:
  - Rigorous models for cybersecurity risk
  - Models for costs and benefits of various cybersecurity technologies
  - Techniques for integrating these models into higher level models that account for other risks and risk management expenditures.

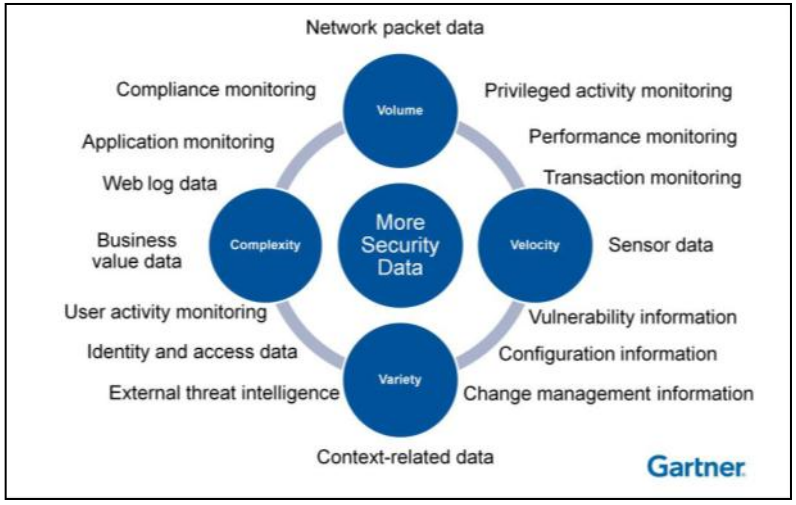
- Technical approach
  - Formulate a two-stage or multi-stage stochastic programming model to numerically identify optimal investment decisions
  - Modeling multiple options to identify an optimal portfolio
  - Ability to model discrete incremental investments over time
  - Flexible representation of breach probabilities and associated risks
  - Extension of value at risk models to evaluate potential losses due to security threats

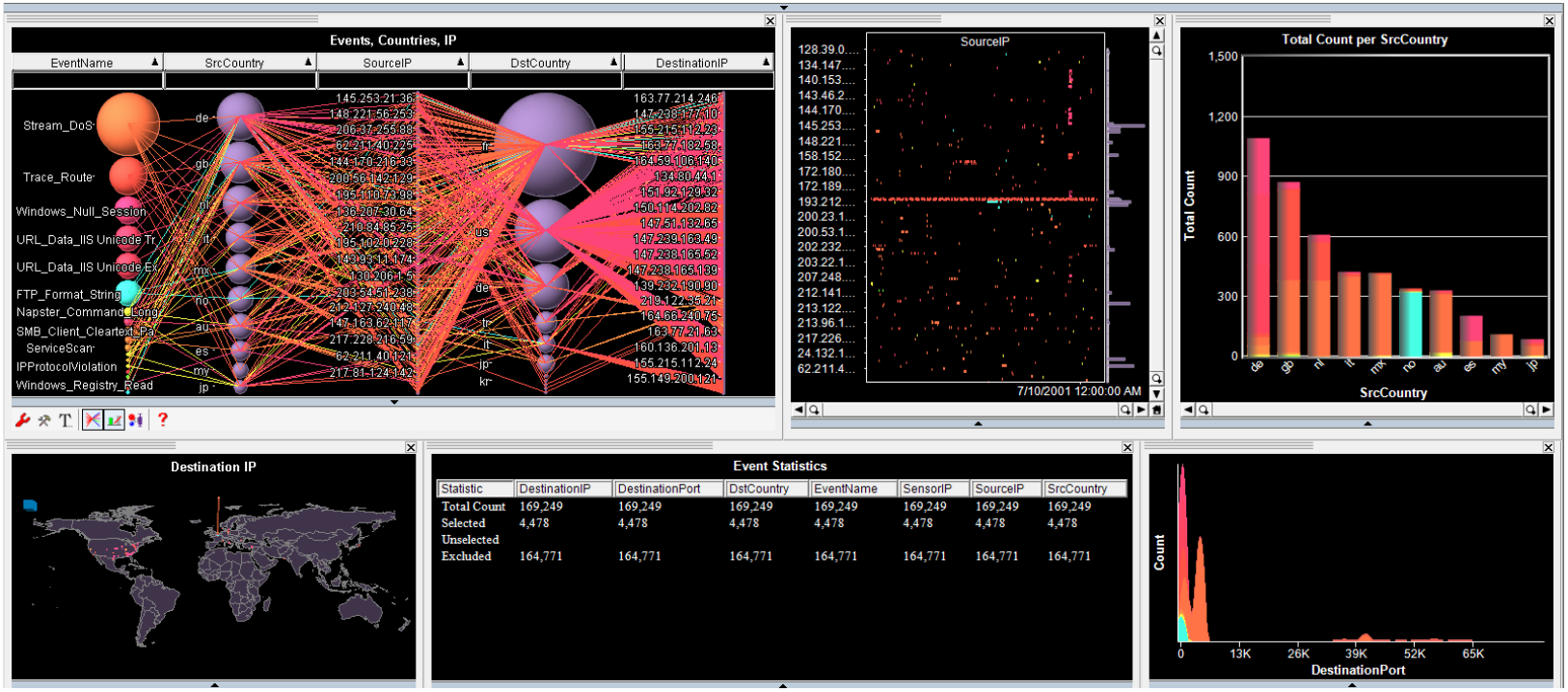


Mass Insight
GLOBAL PARTNERSHIPS

ACSC Research Project #2
Data-Intensive Cybersecurity Monitoring

- Financial services sponsors -- PI's/UMass and BU
- Cybersecurity is a "big data" challenge with significant real-time requirements
- Streaming source filtering, transformation, and integration of multiple data types
- Scalable (M's events/sec) real-time detection and visual analytics
- Archiving, security, resilience, compliance, privacy





Mass Insight
GLOBAL PARTNERSHIPS

Concluding Remarks

- Other potential ACSC research projects in discussion
  - Automation for sharing large-scale machine-readable cybersecurity information
  - Policies and processes for secure mobility in regulated industries
  - Optimization of enterprise security architectures

- "The Computer Security Foundations Symposium (CSF) is an annual conference for researchers in computer security, to examine current theories of security, the formal models that provide a context for those theories, and techniques for verifying security. It was created in 1988 as a workshop of the IEEE Computer Society's Technical Committee on Security and Privacy, in response to a 1986 essay by Don Good entitled "The Foundations of Computer Security—We Need Some." "

  - "Our current logical foundations are inadequate to support a vigorous and growing computer security industry. We need to recognize that problem and solve it. If we do not, we invite serious consequences. Proving that some real systems are secure can help us start building the solid foundations we need. Let's get on with it!"

    Donald I. Good
    The Foundations of Computer Security –We Need Some
    29 September 1986

- Much progress has been made. However, the threats and targets are much larger today. Good's words are still true. The ACSC invites your collaboration as "we get on with it."