DELIVERING CONFIDENCE

Government Keynote

Andy Purdy
Chief Cybersecurity Strategist
CSC Cybersecurity

NDIA 2010 HOMELAND SECURITY SYMPOSIUM & EXHIBITION

September 29, 2010

Summary of Cyber Risk

- The use of innovative technology and interconnected networks in operations improves productivity and efficiency, but also increases the Nation's vulnerability to cyber threats if cybersecurity is not addressed and integrated appropriately.
- A spectrum of malicious actors routinely conducts attacks against the cyber infrastructure using increasingly sophisticated cyber attack tools.
- Because of the interconnected nature of the cyber infrastructure, these attacks could spread quickly and have a debilitating effect.

Cyber News

- "Administration seeks ways to monitor Internet communications"
- "Big cybersecurity contractors turn to little firms for specialized monitoring services"
- "U.S. cybersecurity plans lagging, critics say"
- "Zeus botnets' Achilles' Heel makes infiltration easy"
- "Anti-piracy lawyers' email database leaked after hack"
- "Cyber takes centre stage in Israel's war strategy"
- "Iran confirms massive Stuxnet infection of industrial systems"
- "DOE Funds to Strengthen Grid Cybersecurity"
- "DoD Unveils New Cyber Defense Strategy -- Cyberspace Joins Land, Sea and Air as Fourth Arena of Warfare"

Good news in cyber

- Cyber Storm III
- National Cyber Incident Response Plan (NCIRP)
- White House Cyber Coordinator
- Cyber Command
- National Strategy for Secure Identities
- NIST/DHS – Risk Management and Continuous Monitoring
- DIB Program and IT Pilot
- New Cyber Funding
    - Electric grid security.
    - Innovative cyber solutions
    - Pilots
- Focus
    - Supply chain
    - Secure software
    - Situational awareness/incident response
    - Interoperability
    - Acquisition policy
    - Private sector input

Comprehensive National Cyber Initiative (CNCI)

- Initiative #1. Manage the Federal Enterprise Network as a single network enterprise with Trusted Internet Connections.
- Initiative #2. Deploy an intrusion detection system of sensors across the Federal enterprise.
- Initiative #3. Pursue deployment of intrusion prevention systems across the Federal enterprise.
- Initiative #4: Coordinate and redirect research and development (R&D) efforts.
- Initiative #5. Connect current cyber ops centers to enhance situational awareness.
- Initiative #6. Develop and implement a government-wide cyber counterintelligence (CI) plan.
- Initiative #7. Increase the security of our classified networks.
- Initiative #8. Expand cyber education.
- Initiative #9. Define and develop enduring “leap-ahead” technology, strategies, and programs.
- Initiative #10. Define and develop enduring deterrence strategies and programs.
- Initiative #11. Develop a multi-pronged approach for global supply chain risk management.
- Initiative #12. Define the Federal role for extending cybersecurity into critical infrastructure domains.

Why is the DIB Initiative Important?

- The DIB Cyber Security Program is a major effort to support National Security – It is one of 18 Critical Infrastructures.
- Provides access to threat information and data to proactively implement safeguards throughout the enterprise
  - Information obtained through the DIB will enable providers to more securely support clients in the DoD and Critical Infrastructure
- Strengthens existing Information Risk Management Programs
- Membership in the DIB will highlight the security/trustworthiness of quality providers' services and solutions
- The DIB Pilot requirements are expected to become Federal Acquisition Requirements over the next year

Cyber Attacks Against Critical Infrastructure

Driver for Cybersecurity Services -- Vulnerability of Industrial Control Systems

- The Stuxnet worm, reportedly the most sophisticated malware ever, has targeted Windows PCs that managed large-scale industrial-control systems in manufacturing and utility companies since at least Jan 2010.
- Speculation that Stuxnet was created by a state-sponsored team of programmers, and designed to cripple Iran's Bushehr nuclear reactor.
- Infected at least 30,000 Windows PCs in Iran; Iran's Atomic Energy Organization reportedly met recently to discuss how to remove the malware.
- Microsoft acknowledged that the worm targeted Windows PCs that managed large-scale industrial-control systems in manufacturing and utility companies.
- Those control systems, called SCADA, for "supervisory control and data acquisition," operate everything from power plants and factory machinery to oil pipelines and military installations.

Source:
http://www.computerworld.com/s/article/9188018/Iran_confirms_massive_Stuxnet_infection_of_industrial_systems

“Call it what you will…an international struggle in cyberspace…economic, political, military”

For to win one hundred victories in one hundred battles is not the acme of skill.
To subdue the enemy without fighting is the acme of skill.

Sun Tzu

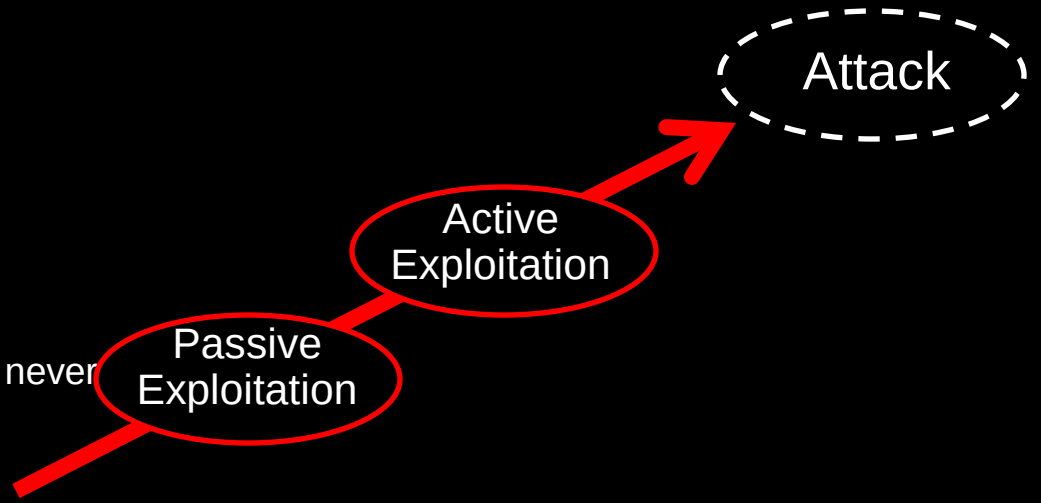
A Three Stage Escalation…we are engaged in Stage 2

Stage 1: Passive Exploitation

- Reconnaissance
- Mapping, Code Injection
- Find weaknesses

Stage 2: Active Exploitation

- Steal blueprints
- Create Disinformation
- Success would mean that there may never be a need to go to Attack

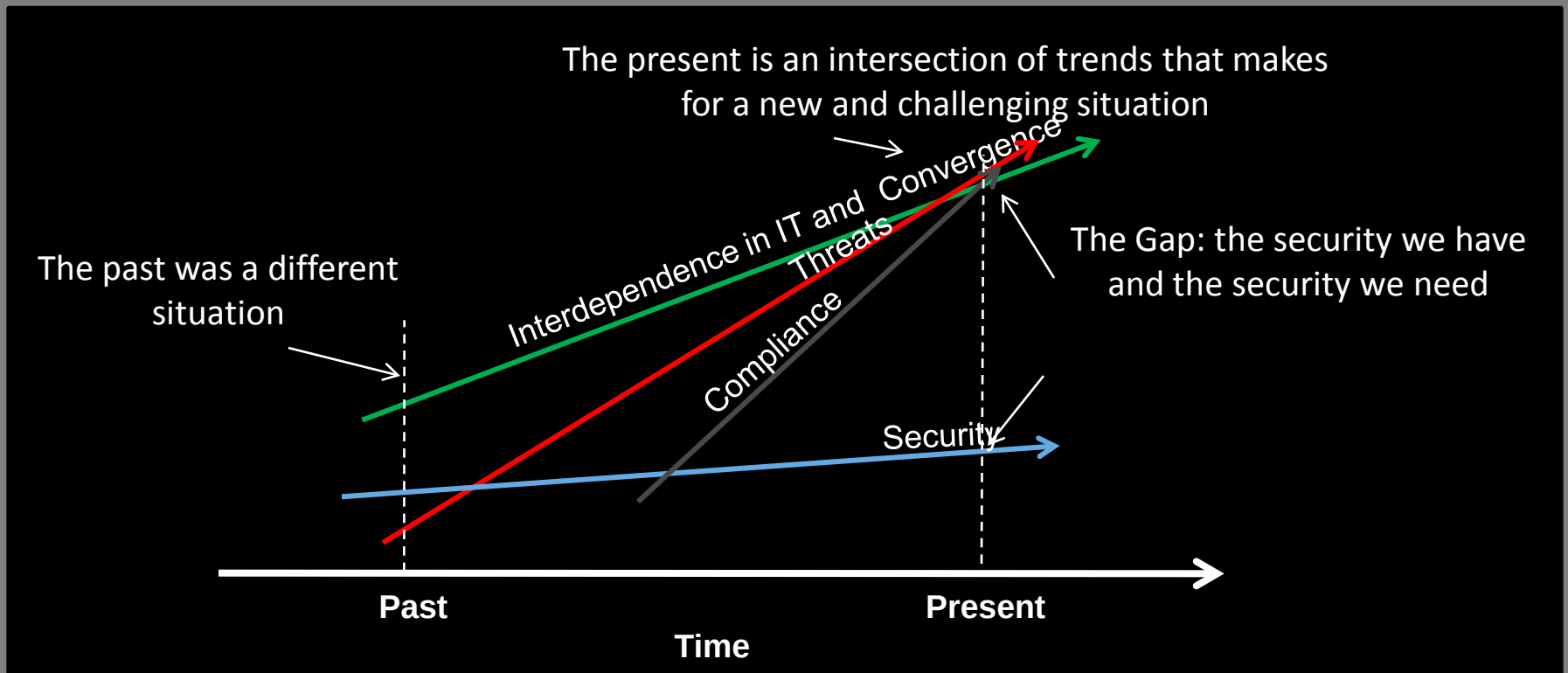


Stage 3: Attack

- Take down a utility
- Disrupt a supply chain
- Create financial mis-trust

"It's asymmetric because…
those intent on harm: are everywhere, may not be an organization at all, unconstrained by geo-political boundaries, can't pin attribution with certainty, motives are boundless, and groups combine not unlike business partners in a commercial market"

What's different between then and now…



It may be that the question is not of ROI – but do you want to stay in business – a corporate and a national question

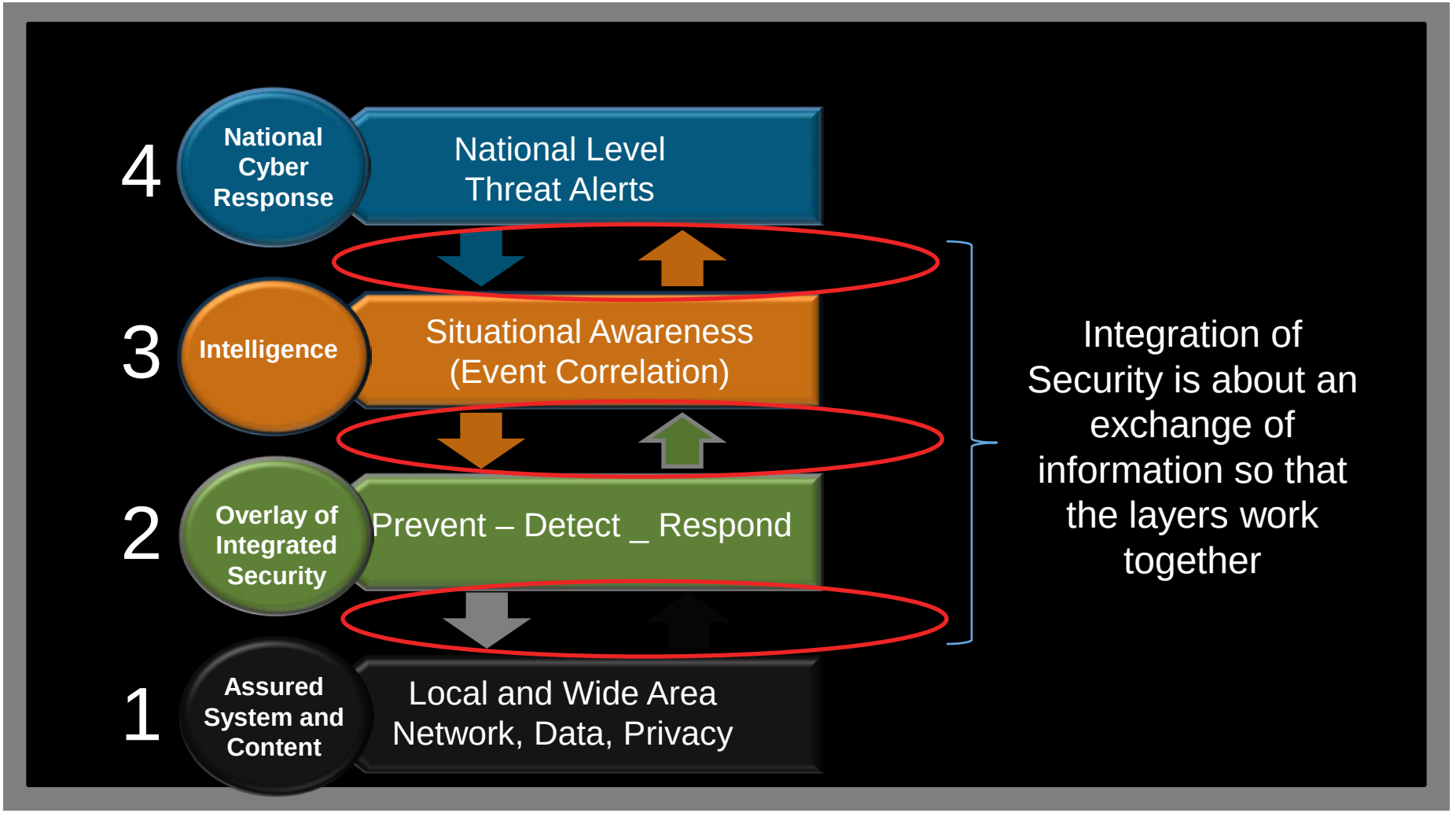
Lessons we should understand…

- Witnessing the depletion -- loss of competitive advantage
- It's a new world – new generation of threats
- Adversaries are in our systems
- Compliance (penalties) more stringent – not less
- Answers: Security must be designed in (architected)
- Bolt-on security insufficient to the present task
- Stage 2 (Active Exploit) is here to stay
- You will not hear a bang – maybe a hiss (air escaping); maybe nothing
- Time to wake up to this reality

“The Security Stack”

Designing Security In: "The Security Stack"

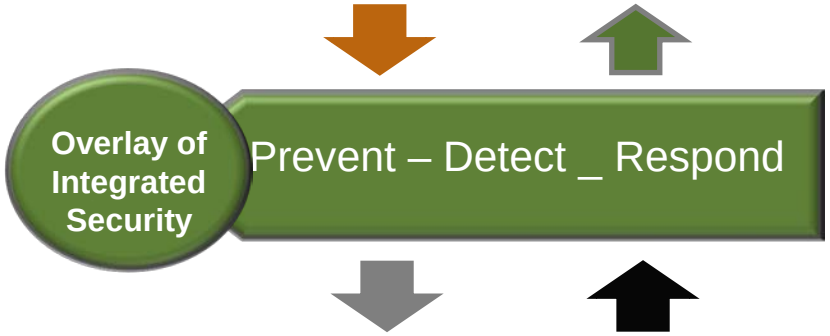
Measuring up - to a new generation of threats



The Cybersecurity Stack (Layer 1)

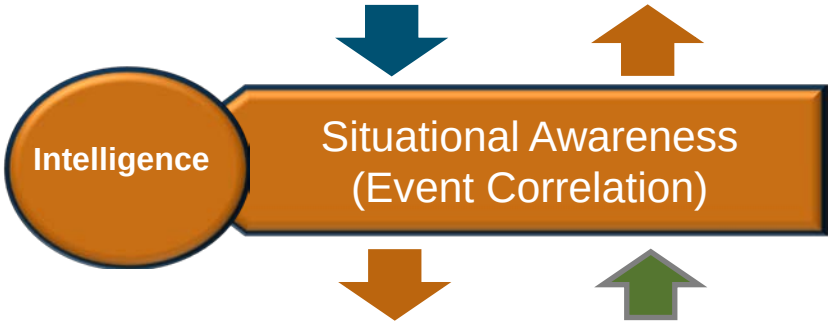
- Architecting (designing-in) the security
  - Enclave Isolation
  - Configuration Management Data Base
  - Endpoint Protection
- Privacy Requirements
  - Data Classification
  - Encryption
- Takes security solution engineers
  - Working with our solution architects
- Requires integration with Layer 2 functions
  - Unauthorized Configuration Information passed up to L2

The Cybersecurity Stack (Layer 2)



- Integrating the security overlay
  - Firewalls
  - Security Manager
  - Intrusion Detection – Prevention
  - Data Loss
- Takes security solution engineers
  - Working with our solution architects
- Requires integration with Layers 1&3 functions
  - Example: Unauthorized Configuration Information passed up to L2

The Cybersecurity Stack (Layer 3)



- Integrating situational awareness
  - Event Correlation
  - Incident Management
  - Threat Indices - External
- Takes security solution engineers
  - Working with our solution architects
- Requires integration with Layers 2&4 functions
  - Example: Log information looking at trends, multi-threaded attacks, signatures, integration with external sources of threats (indices)

The Cybersecurity Stack (Layer 4)

- Integrating situational awareness with Government – for critical infrastructure companies
  - Threat Indices – External
- Requires integration with Layer 3 functions
  - Example: government provided threat indices

A Strategic View of ICT Security

- There is no real separation in cyberspace; we share a common environment with allies, partners, adversaries, and competitors.
- It is important to understand computer network defense, and be informed by exploitation and attack.
- Security is more about architecture and integration than about deployment of more products to build perimeter defenses.

Public Sector aggressively investing in Cyber Solutions driven by increase in severity and number of attacks.

The U.S. public sector has seen an increased investment in cyber security technologies and has begun to coordinate cybersecurity activities, set cyber security R&D goals and create frameworks for public/private partnerships.

Drivers	• Exponential increase of data flows over government networks. • U.S. adversaries perceive our dependence on information technology and our cybersecurity weakness as exploitable. • Increased endpoint security risks from mobilized workforce. • Confidential information leaks via Web 2.0 applications. • Increase number of data breach incidents. • Increased use of virtualization technologies such as cloud computing and open source applications.
Public/Private Partnerships	• Aligning of national defense with critical infrastructure. • Private sector designs & operates public sector infrastructure. • Public sector must defend infrastructure. • Private sector reluctant to share information due to threats against their intellectual property due to Freedom of Information Act. • Industry also needs the government to protect their competitive, proprietary data for economic advantage.

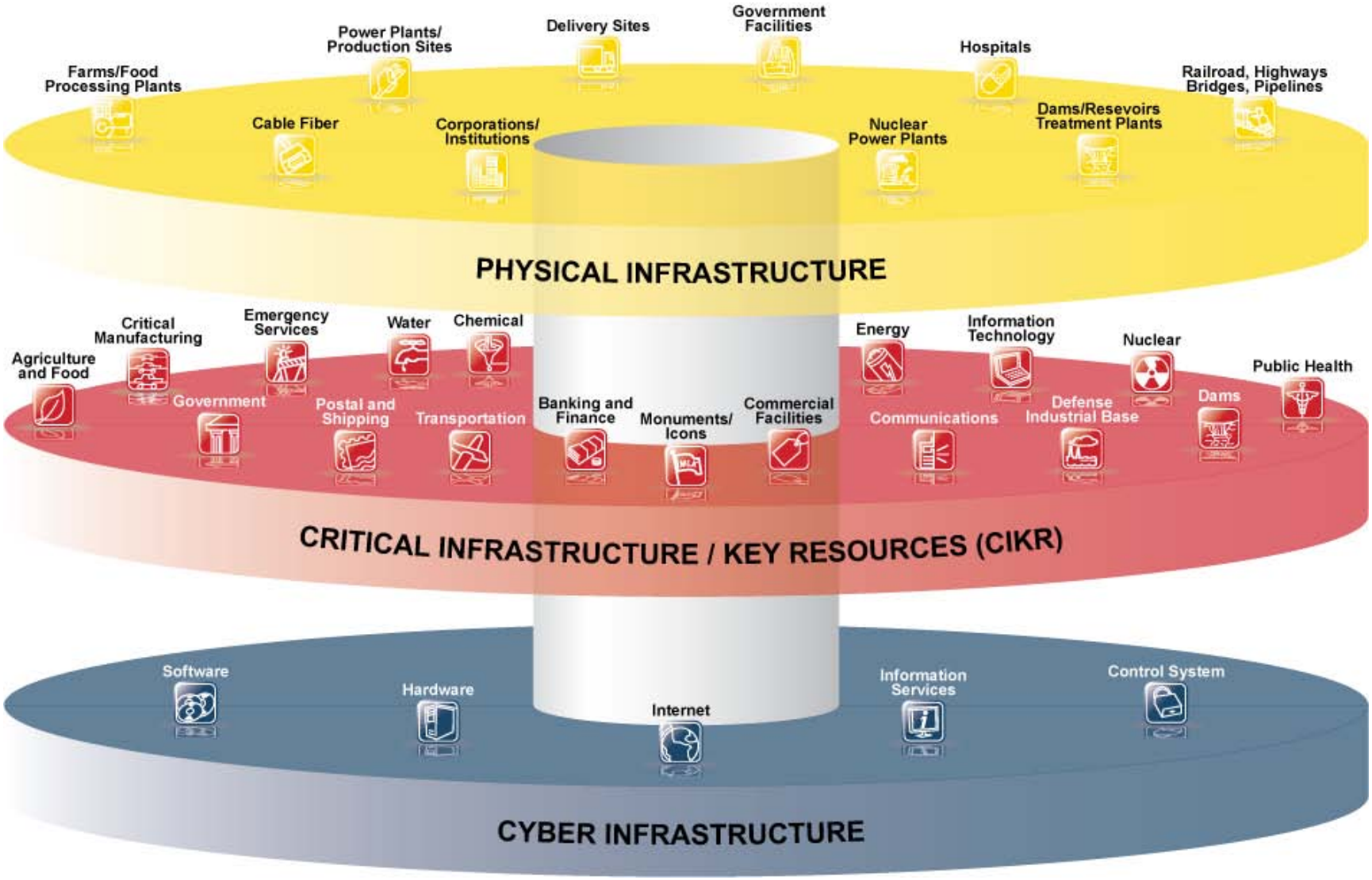
Cybersecurity – a National Security Imperative and Global Business Issue

- Nations and critical infrastructure owners and operators are dependent on Cyber for national security, economic well-being, public safety and law enforcement, and privacy.
- Major companies must ensure the resiliency of their operations, protect their reputations and the privacy of their customers, differentiate their brand, and meet compliance obligations.
- Innovative technologies and information assurance strategies must be implemented by government and private companies through fully integrated, end-to-end cyber solutions

Public Policy Challenge

- Nations are dependent on cyber for national security, economic well-being, public safety, and law enforcement
- Risk is real but not visible and obvious
- Authority/control is spread among multiple entities in the public and private sectors
- ICT is international
- Individuals and organizations are reactive and tactical, not proactive and strategic
- We do not learn lessons from the past

Cyber infrastructure underpins critical elements of CIKR



What is needed nationally and internationally?

A strategic approach to facilitate public/private collaboration and information sharing to set requirements, and resource, execute, and track progress on national strategic priorities:

- ICT risk;
- ICT preparedness;
- Malicious activity and cyber crime; and
- Research and development.

How should the challenge of ICT risk and preparedness be addressed?

- Stakeholders at the organizational, national ,and int'l levels must work together
  - to identify critical functions,
  - assess and mitigate risk, and
  - plan, and build capacity for, response and recovery
- Use standards to drive risk reduction
- Exercise to identify gaps and improve
- Pursue innovation
- Use this process to identify requirements to drive resource allocation for risk mitigation, response preparedness, and research and development

What do we need to do? How are we doing?

1. Private sector needs a seat at the table of decision-making.

   - Need representatives to the IPC and IPC sub-working groups.

2. Identify strategic priorities for public/private collaboration informed by input from private sector and government representatives:
   - Cyber risk;
   - Cyber preparedness;
   - Malicious activity and cyber crime; and
   - Research and development.

3. Each priority requires goals, objectives, and corresponding metrics and milestones.
   - Helps in setting resource requirements.
   - Promotes accountability by government (Executive and Legislature) and by private sector.
   - Makes it possible to track progress and inform areas of improvement.

4. International agenda should further strategic cyber priorities

Cyber Risk

- Nation's threat paradigm needs to be replaced by a risk paradigm (threat, vulnerabilities, and consequences);
- We need a national cyber risk assessment that spells out what the nation needs to worry about and what we need to do about it;
- Using a risk focus, expand the NIE (threat) model of broad-based government participation, to include private sector.

Cyber Preparedness

- Set requirements for situational awareness and a common operating picture for government and critical infrastructure
- Set requirements for a a public-private collaborative framework to address cyber incidents:
  - Analysis
  - Response
  - Recovery

Research and Development

- The nation must develop a national cyber R&D agenda to better assess and mitigate risk, enhance preparedness, and address the long-term hard problems we face in cyberspace
- The agenda must be informed by government and private sector, academia, and our closest allies.

Malicious Activity

- We must act strategically and proactively
- Malicious activity is a key component of ICT risk -- one part of a continuum of risk that the nation faces from terrorists, sophisticated hackers and hacktivists, organized criminal groups, and nation states (and those working for them).
- Law enforcement must work across government and with the private sector to prioritize action and resources, track progress, and impact malicious activity to reduce risk.
- Accountability is key to progress.

Malicious Activity/Cyber Crime

- U.S. must work nationally and internationally to address the underlying problem that there are virtually no consequences for malicious activity in cyberspace.
- Government and private sector should partner to collect and share data on the most significant malicious actors & enablers
- Coordinate efforts to shut them down and reduce frequency, impact, and risk of malicious cyber activity
- Mitigate the circumstances and vulnerabilities that allow them to operate
- Encourage private lawsuits as a complement to law enforcement

Protecting Your Organization, Clients, and Customers

- Improve your enterprise using:
  - an architectural approach,
  - assess it against appropriate standards,
  - implement a risk management program including continuous monitoring technology, and
  - subject your enterprise to periodic, independent assessments.
- Use lessons learned from Advanced Persistent Threats (APTs) and other sophisticated attackers to strengthen active defense
- If possible, join the Defense Industrial Base Pilot Program
- Work in public-private partnerships (e.g., ISACs, Sector Coordinating Councils, InfraGard, Electronic Crimes Task Force, National Cyber Forensics and Training Alliance, and associations) to strategically collaborate and share information about threat and risk

Andy Purdy
dpurdy@csc.com

http://www.csc.com/cybersecurity