DELIVERING CONFIDENCE

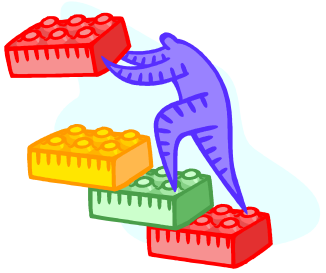
STRATEGIES FOR SECURING THE ENTERPRISE

Paul Croll
Fellow
March 2, 2011

Enterprise Risk Management – Balancing Assurance Costs

- NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems describes risk management for IT systems as a process that balances the operational and economic costs of protective measures to achieve mission-essential security capabilities
- NIST Special Publication 800-27, Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A, recognizes that elimination of all risk is not cost-effective
  - *A cost-benefit analysis should be conducted for each proposed control. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Benefits include more than just prevention of monetary loss; for example, controls may be essential for maintaining public trust and confidence*

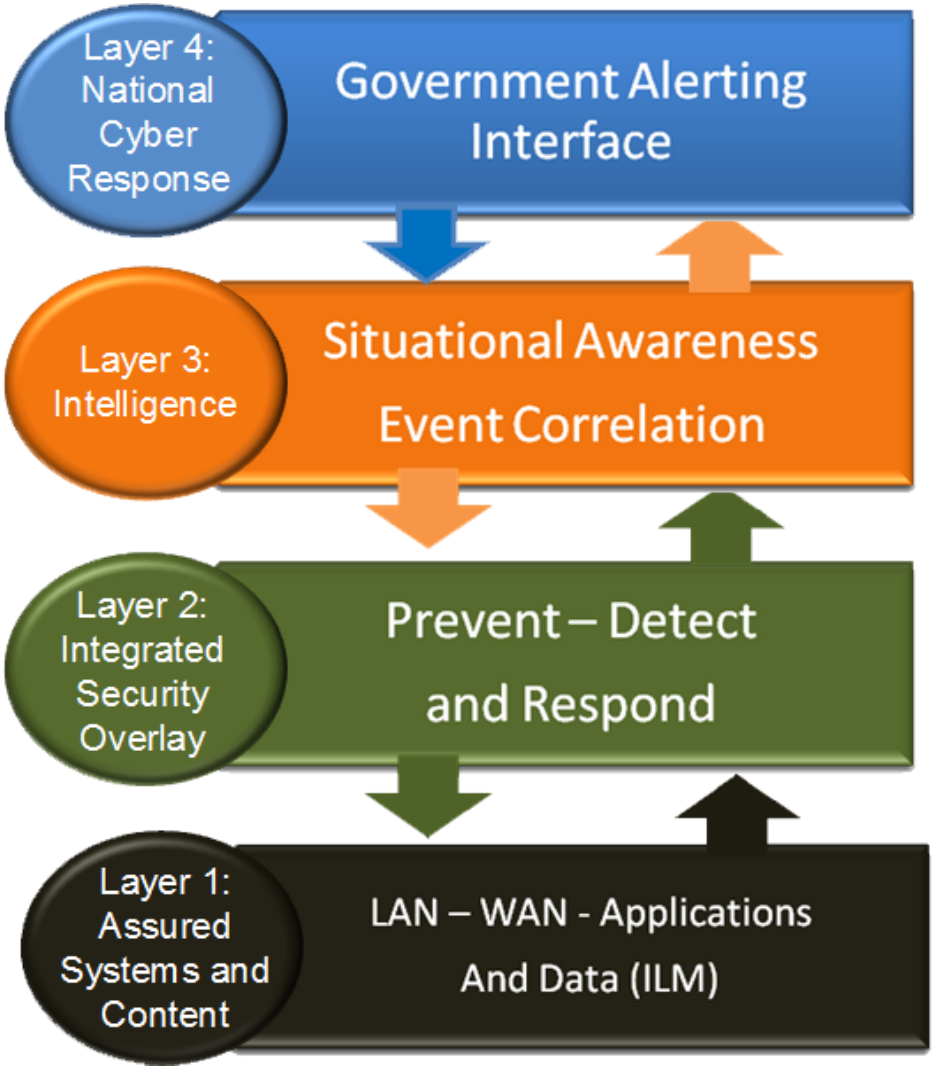
Principle 5: Reduce risk to an acceptable level



Risk Hierarchy for Enterprise Security

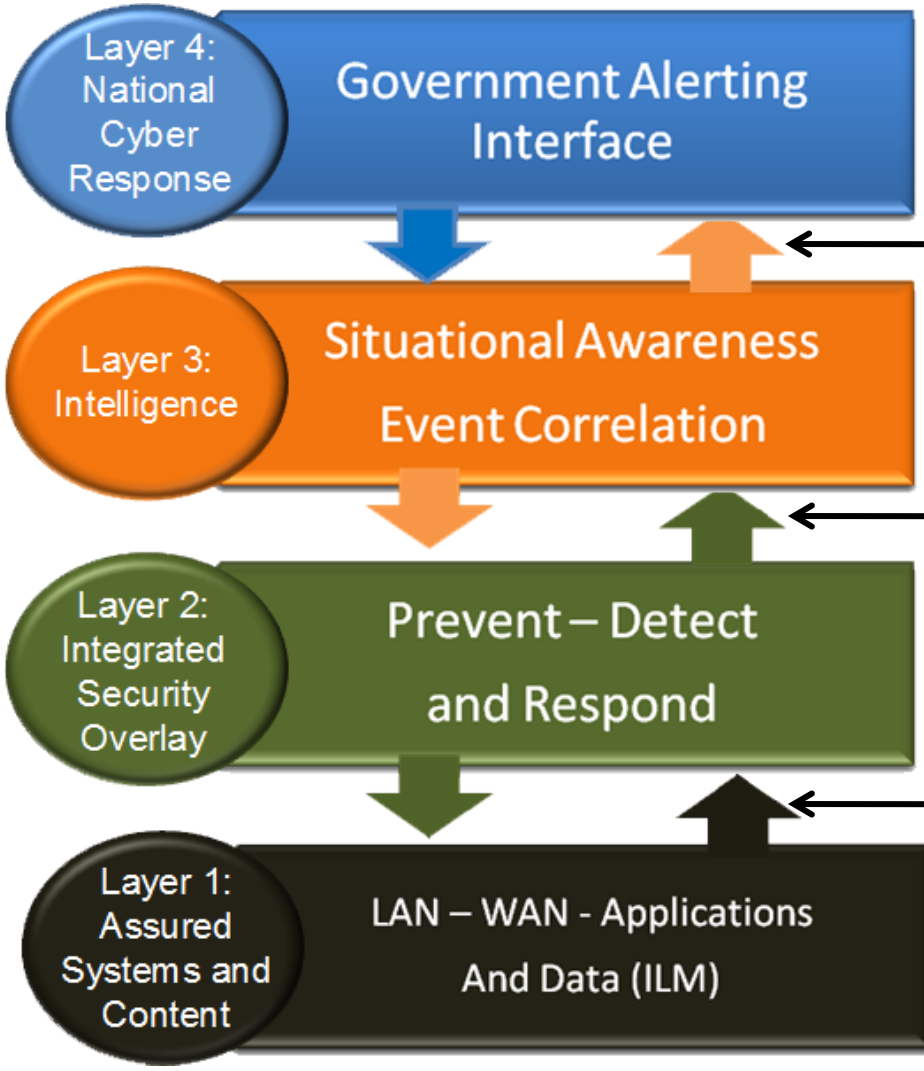
- Legal and Regulatory Risk
  - This class of risk addresses risks associated with failures regarding compliance with legal or regulatory requirements
  - Consequences may include fines, civil or criminal prosecution, prohibitions against provision of products to the market place.
- Operational Risk
  - This class of risk addresses both external and internal risk
    - External risks associated with failures of provided products in their operational environments,
    - Internal risks associated with failures in the engineering processes producing such products.
  - Consequences may include delivered exploitable vulnerabilities that result in harm to users, their systems, or their data
- Reputational Risk
  - This class of risk is linked with legal and regulatory, operational, and competitive risk
  - It addresses risks associated with damages to the organization's reputation in the market place resulting from legal and regulatory breaches and operational failures
  - Consequences include loss of standing in the market place and mistrust on the part of current and potential customers.
- Competitive Risk
  - This class of risk addresses risks associated with loss of stature with respect to competitors.
  - Consequences include loss of market share and potential difficulty entering new markets.
- Financial Risk
  - This class of risk addresses risks associated with monetary loss
  - Consequences include loss of revenue, negative impact on stock prices, and diminishing shareholder confidence.
- Strategic Risk
  - This class of risk is linked with all the other risk classes below it in the hierarchy
  - It addresses risks associated with failures to meet the strategic goals and objectives of the organization

A Model for Closing the Gap: The Security Stack



- **Layer 4:** Public-private interface of critical security information and remediation.
- **Layer 3:** The external intelligence component of the threat landscape that needs to be distributed across the environment at all levels.
- **Layer 2:** Holistically managing network security - distributing and acting on threat data.
- **Layer 1:** Data classification-separation, allowing secure operation under a variety of risk profiles in different business verticals.

A Model for Closing the Gap: Realizing The Security Stack



Government threat information – integrated into the SOC

Threat intelligence exchanged for critical infrastructures

A 24x7 SOC with global presence at 4 levels

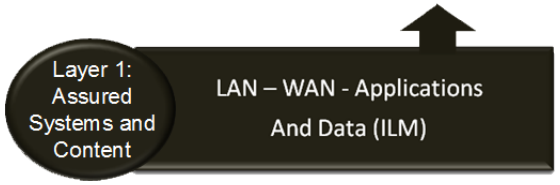
Sensor (logs) info exchanged, defenses adjusted

Security systems integrated by security experts

Monitor configuration – adjust access accordingly

Security architected as part of the software, network

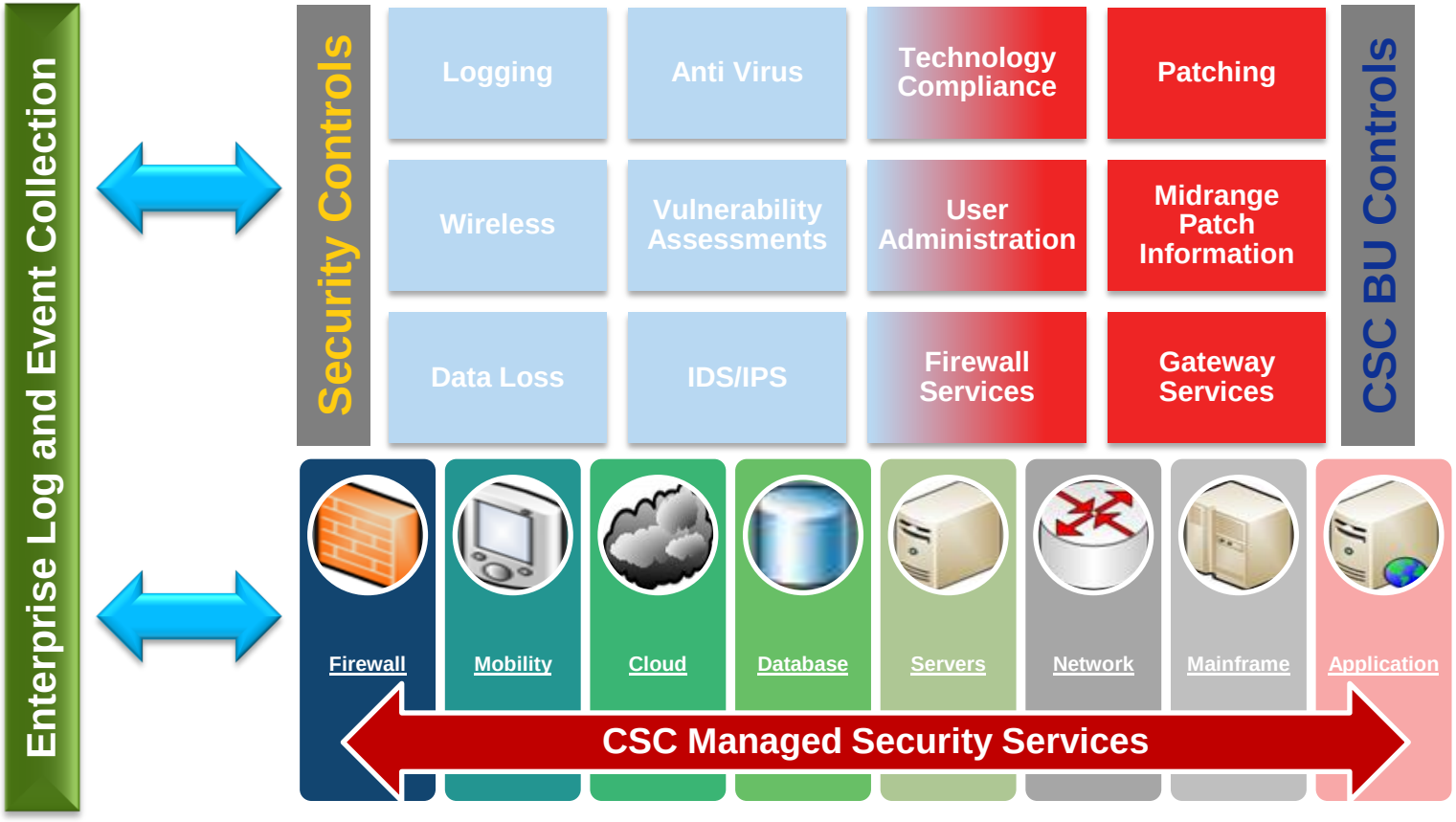
Layer 1: Assured Systems and Content



- The set of information-communications technologies (ICT) architected and designed to operate securely within an appropriate cyber-threat environment
- Layer 1 employs technologies or methods such as data encryption or use of software assurance methodologies
- A disciplined method for configuration management is also essential
- Another central concept for this layer is the use of standards to achieve rigor in the processes for assured systems and content..
- The information exchange between Layers 1 and 2 can be extensive and requires that information go from machine to machine without human intervention to achieve speed in detecting anomalous behavior

Example – Enterprise Logging

Challenge - Develop an enterprise logging solution ensuring network, application and system logs are centrally collected, unaltered and stored.

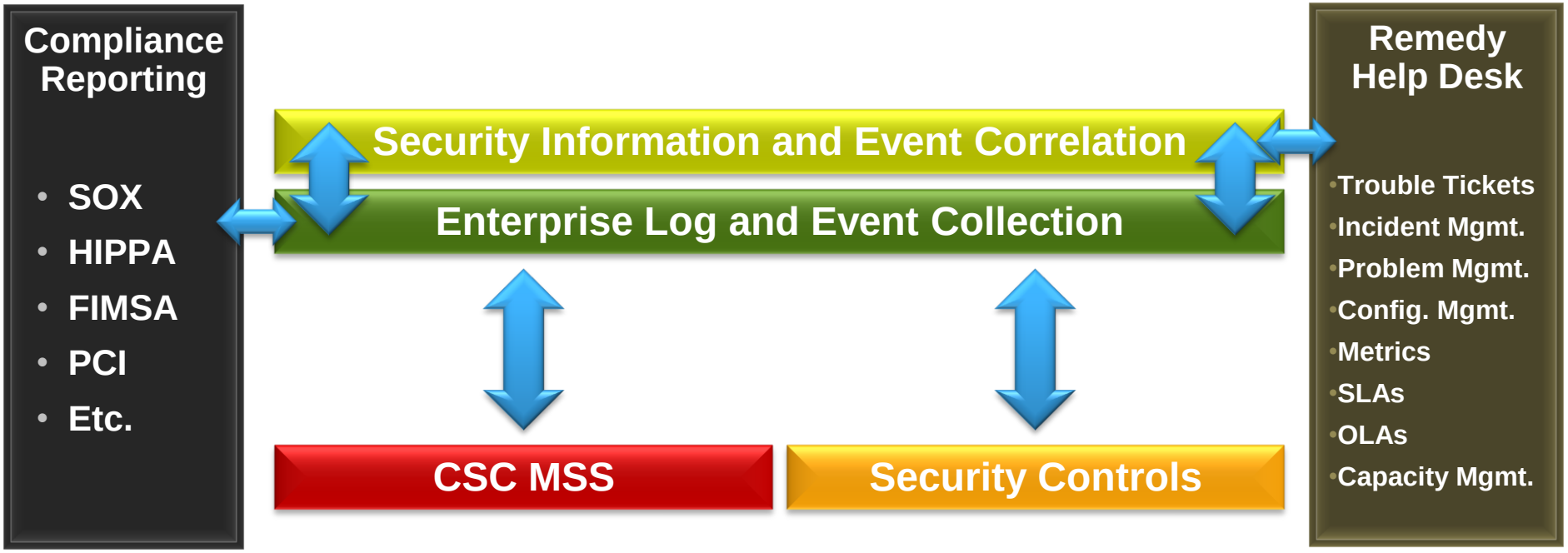


Layer 2 – Integrated Security Overlay

- Layer 2 is the traditional bolt-on “security” layer as we know it today
- It comprises several control planes across both the network and application layers
- It includes Security industry “point solutions,” where each vendor’s solution independently addresses problems at specific points in the architecture
- Information exchange among these security elements is of key importance, and they are confounded by a lack of interoperability (as in incompatible data formats from different sensors) that ultimately slow the process of correlating information needed in detection efforts

Example – Information & Event Correlation

Challenge - Gather and correlate information and events across enterprise infrastructure, reducing support costs and improving the ability to identify and respond to the evolving threat landscape including Advanced Persistent Threats

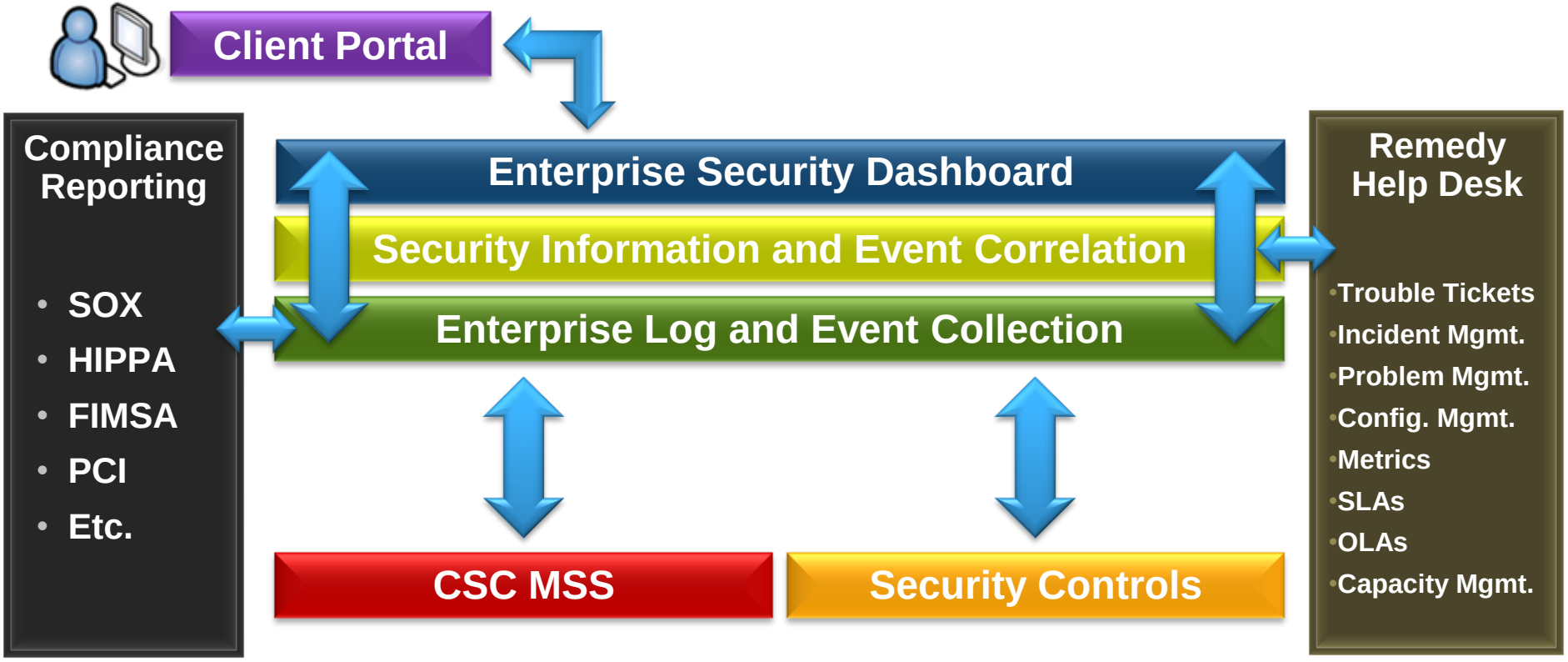


Layer 3 – Intelligence

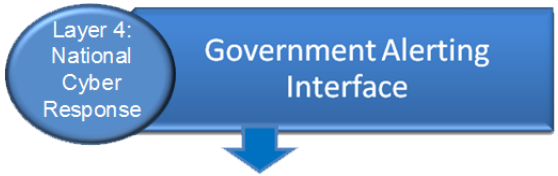
- The anonymity of the Internet and certain shortcomings of TCP/IP make it difficult to learn about those who would do harm. This is the problem of attribution
- We need better intelligence regarding what is going on inside the network perimeter and what is taking place outside the network, beyond our immediate control. This, in essence, is situational awareness
- Situational awareness suffers from the multitude of languages and mechanisms used to convey information
  - We need communications mechanisms that allow us to combine data sources easily
- Situational awareness is the first step toward automating defensive systems that will operate in “Internet time.”

Example – Enterprise Security Dashboard

Challenge – Provide SOC staff and the client visibility regarding their risk, threat, vulnerability and compliance posture

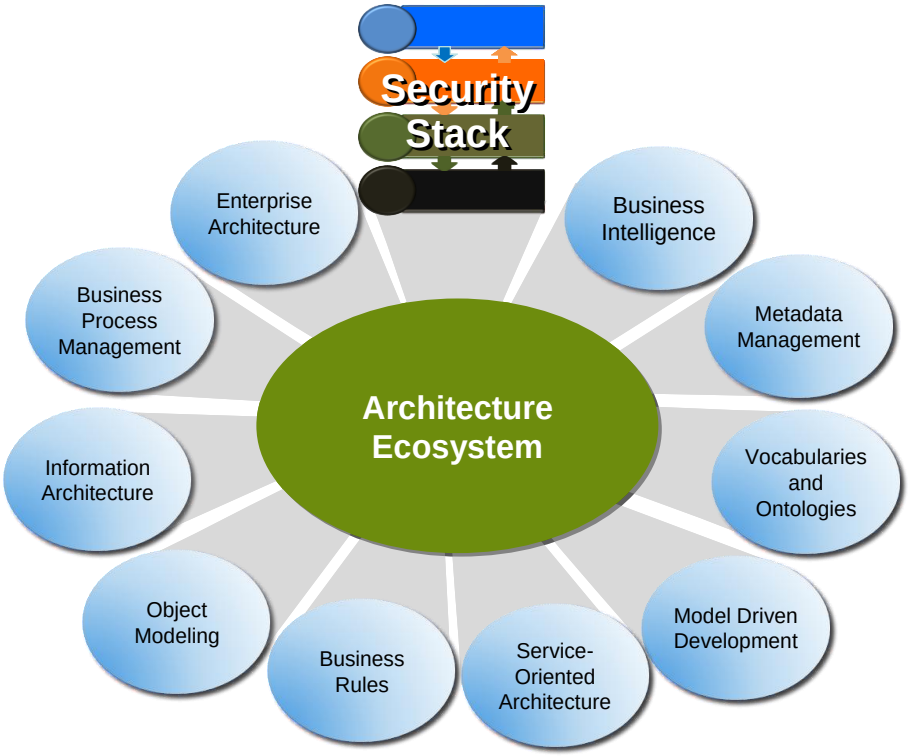


Layer 4 – National Cyber Response



- Layer 4 represents the intersection of national security interests with the interests of the private sector
- Layer 4 is distinct from other layers focusing not on networks, but on a bridge between the private and public sectors for specific functions consistent with the role of government as protector
  - Threats operate in “Internet time”
  - The current means of exchanging threat information between government and critical infrastructures continues to operate in “bureaucratic time”
  - In order to protect National critical infrastructures such as telecommunications networks, the power grid, and air space exchanges of threat information cannot wait for bureaucratic time

The Architectural Context for Enterprise Security



- The Security Stack is a part of an architecture ecosystem – a collection of architectural views (rules, enterprise architecture, data, metadata and now *security*) that collectively specify all the elements of a system and its environment
- The security stack elements described above affect architectural elements of other views, and the elements of the other views affect the security stack elements
- This interdependence helps assure that security is built in and not bolted on

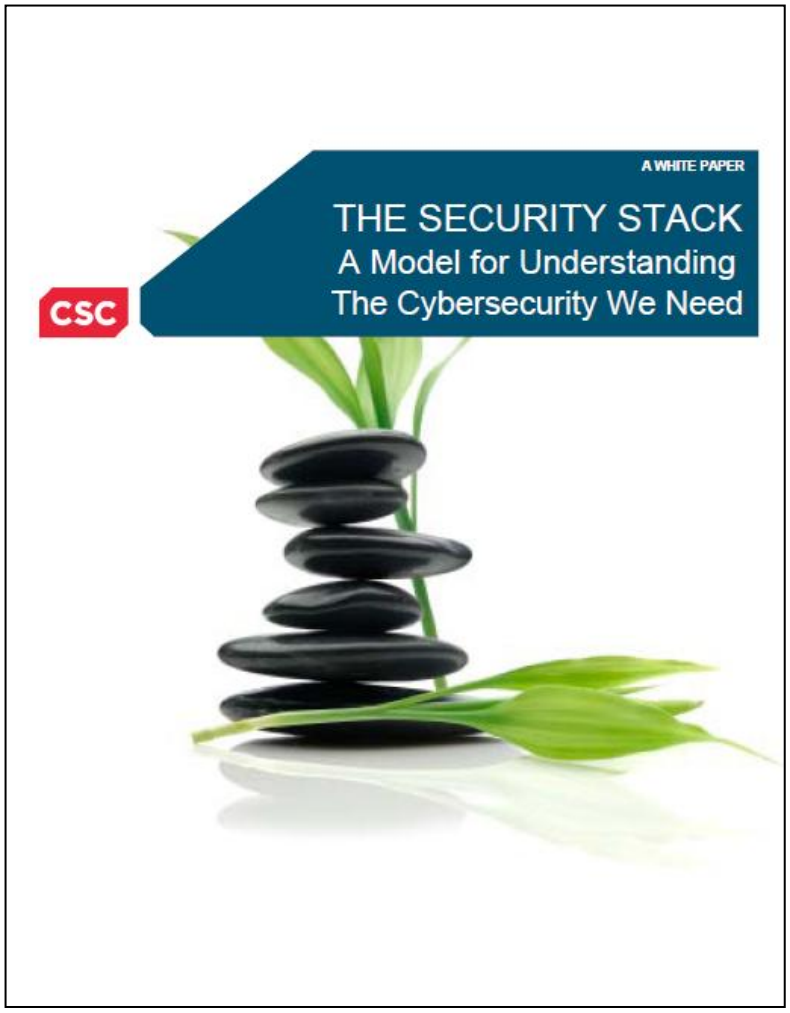
Questions

Paul R. Croll
CSC
10721 Combs Drive
King George, VA 22485-5824

Phone: +1 540.644.6224

Fax: +1 540.663.0276

e-mail: pcroll@csc.com



http://www.csc.com/cybersecurity/blog/45966/53330-download_our_new_security_stack_white_paper