2011 Cyber Security and the Advanced Persistent Threat – A Holistic View

Thomas Varney
Cybersecurity & Privacy
IBM Global Business Services

Agenda

- The Threat We Face
- A View to Security
- Addressing the Four Big Problem Areas
  - Identity & Access Management
  - Application Security
  - Cyber Situational Awareness & Vulnerability Management
  - Continuous Monitoring

Security on a Smarter Planet

The planet is getting more
Instrumented, **Interconnected** and **Intelligent**.

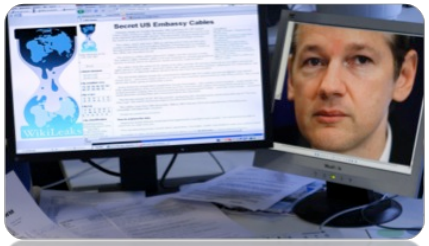
162 million
Almost 162 million smart phones were sold in 2008, surpassing laptop sales for the first time.

90%
Nearly 90% of innovation in automobiles is related to software and electronics systems.

1 trillion
Soon, there will be 1 trillion connected devices in the world, constituting an “internet of things.”

Strategic Change 1: The impact and visibility of recent breaches calls into question the effectiveness of traditional security measures

Internal abuse of key sensitive information

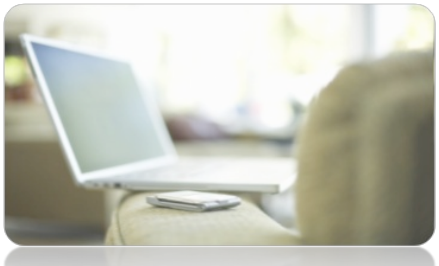


In spite of significant security policies, a single internal breach by an authorized user resulted in tens of thousands of classified records of the **US Army** leaked over Wikileaks**.** Impact to the Army is close to $100M

Complexity of malware, growth of advanced persistent threat

Stuxnet turned up in industrial programs around the world. The sophistication of the malware has led to beliefs that it was developed by a team of over 30 programmers and remained undetected for months on the targeted environment. Targeted to make subtle undetected changes to process controllers to effect uranium refinement

Business continuity interruption and brand image impact



Epsilon, which sends 40B e-mails annually on behalf of more than 2,500 clients, said a subset of its clients' customer information was compromised by a data breach. Several prominent banks and retailers acknowledged that their customers' information might be at risk

Strategic Change 2: Security challenges are impacting innovation

External threats	Internal threats	Compliance
Sharp rise in external attacks from non-traditional sources	Ongoing risk of careless and malicious insider behavior	Growing need to address an increasing number of mandates
▪ Cyber attacks ▪ Organized crime ▪ Corporate espionage ▪ State-sponsored attacks ▪ Social engineering	▪ Administrative mistakes ▪ Careless inside behavior ▪ Internal breaches ▪ Disgruntled employee actions ▪ Mix of private / corporate data	▪ National regulations ▪ Industry standards ▪ Local mandates

Impacting innovation

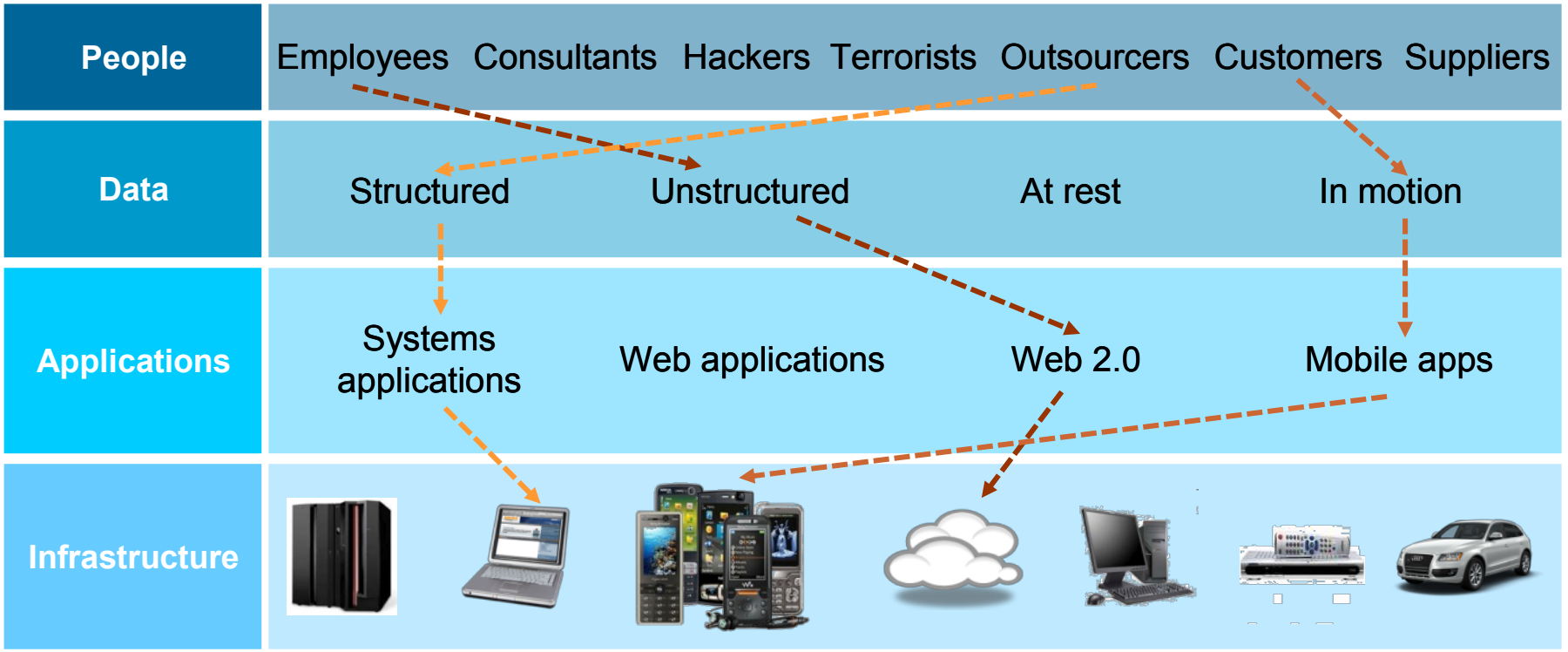
Mobility

Cloud / Virtualization

Social Business

Business Intelligence

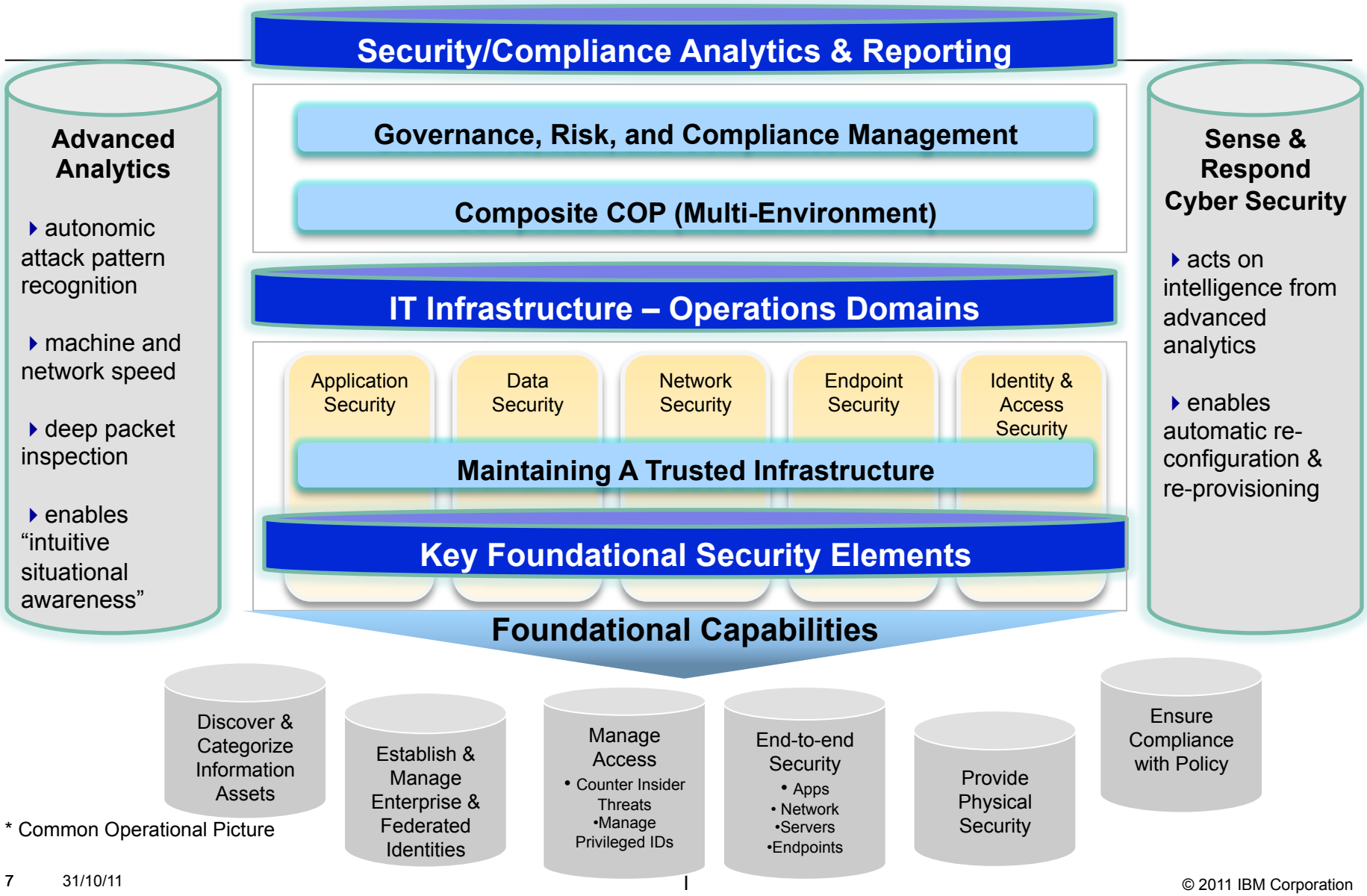
Strategic Change 3: The attack surface for a typical business is growing at an exponential rate



- **77%** of firms feel cyber-attacks harder to detect and **34%** low confidence to prevent
- **75%** felt effectiveness would increase with end-to-end solutions

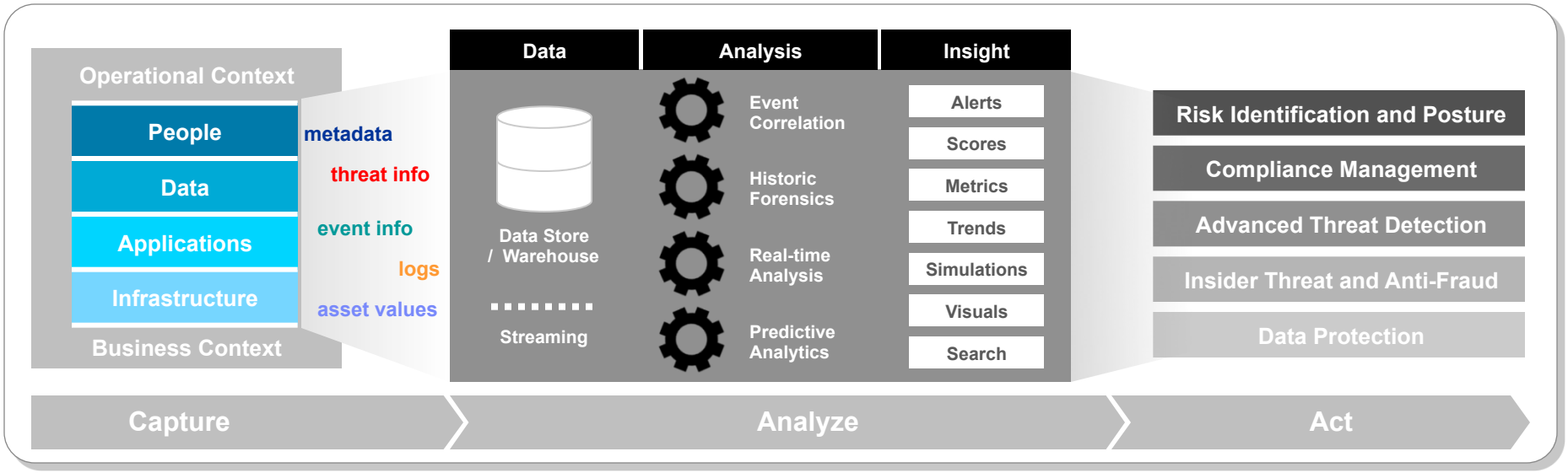
Source: Ponemon Institute, June 2011

Fitting it all together to provide dynamic Cyber Security



* Common Operational Picture

Security intelligence simplifies complex security problems and provides comprehensive business insight through the integration of optimized security controls and contextual information about people, data, applications, and infrastructure – using deep analytics to identify, predict, and remediate IT threats and enterprise risk



Intelligence is the Key

Addressing the Four Big Problems Areas

- **ID & Access Management**
- **Application Security**
- **Cyber SA & Vulnerability Management**
- **Continuous Monitoring**

1st Point of pain - If you cannot control your network, your adversaries will.

.

Threat Management

Data Protection

Cyber Security

Mission Assurance

Identity and Access Management (IdAM): used to positively identify a person or device on a network and manage that entity's access to the system resources based on the established identity. It must be in concert w/ NSTIS's Identity Ecosystem and HSPD 12. Characteristics include:

- Established business process to manage personnel/devices and their associated digital identity from hire/acquisition through retire (end-to-end life cycle)
- Integrated technologies that address the spectrum of scenarios in each stage of the identity life cycle
- Policies relating to the constraints and standards required to comply with regulations and business best practices
- Processes that specify the sequence of steps required to complete business tasks or functions
- Technologies that automate process, and enforce policies, to efficiently and accurately enhance business objectives
- The policy, process, and technology that have a built-in feedback loop to ensure compliance, effectiveness, & efficiency

Confidentiality

Integrity

Availability

2nd Point of pain - Applications now provide the power and flexibility for performance. Are yours as safe as they are effective?

Threat Management

Data Protection

Cyber Security

Mission Assurance

Application Security. used throughout an application's life-cycle to prevent exceptions in the security policy of an application or the underlying system (vulnerabilities) through flaws in the design, development, deployment, upgrade, or maintenance of the application. Characteristics include:

- Standardized and automated systems development life cycle methodology which includes assessing code, application security and controls
- Well defined enterprise assets, including what each application does with respect to the enterprise assets, a security profile for each application, identifying and prioritizing potential threats, and documenting adverse events and the actions taken in each case
- Continuous web application testing
- ERP security and controls
- SOA security strategy and architecture
- Application security services for cloud

Confidentiality

Integrity

Availability

3d Point of Pain - Knowledge of what and who are on your network, combined with the ability to effectively respond to problems give the assurance you control your cyber destiny.

Threat Management

Data Protection

Cyber Security

Mission Assurance

Cyber Situational Awareness & Vulnerability Management.

Provides visibility of all assets found on the organizational network, their status at any given moment, what may be threatening these assets or the data contained on them, and leads to machine speed actions that can lower the risk to the organization. Characteristics include:

- Full and dynamic inventory of network assets
- Monitor the security status of all assets and data
- Monitor the status of all patch and non-patch actions
- Prioritize remedial actions that need to be taken
- Oversee vulnerability remediation
- Execute vulnerability remedation

Confidentiality

Integrity

Availability

4th Point of Pain - Continuous Monitoring has the single biggest potential for achieving real cybersecurity; ALL Federal clients need this.

Threat Management

Data Protection

Cyber Security

Mission Assurance

Continuous Monitoring: detect and track governance, compliance, and risk associated with the security of an organization's information and technology through real time observation. Characteristics include:

- Unified policies, procedures, and guidelines
- Improved situational awareness through dash board reporting
- Rigorous metrics to determine effective defense against vulnerabilities & attacks
- Ongoing monitoring of activities, people, data, and programs rather than a static, snap shot in time
- Strategies that collect data, develop information and use knowledge to develop and maintain a dynamic defense
- Examining 100% of transactions and data processed in monitored applications and databases
- Secure products and architecture by design, rather than add-on

Confidentiality

Integrity

Availability

DISCUSSION

Thomas Varney
Cybersecurity & Privacy
IBM Global Business Services