IBMSecurity Symposium

Intelligence | Integration | Expertise

Security- New extensions

Vaidyanathan Iyer(Vaidy)

BUE IBM Security Systems

ISA

Top Information Security Trends -2012

1. Identity Access Management

2. Data Security

3. Application Security

4. External Threats – Worms, Trojans, Viruses

5. Aligning IT security with business

6. User Training

7. IT Security Staff training

8. Business Continuity and disaster planning

9. Cloud Security

10. Regulatory compliance

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks

DATA EXPLOSION

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere
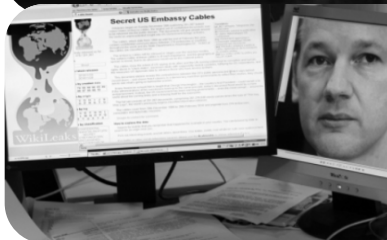
CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared
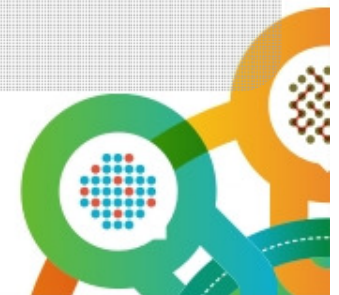
EVERYTHING IS EVERYWHERE

Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more
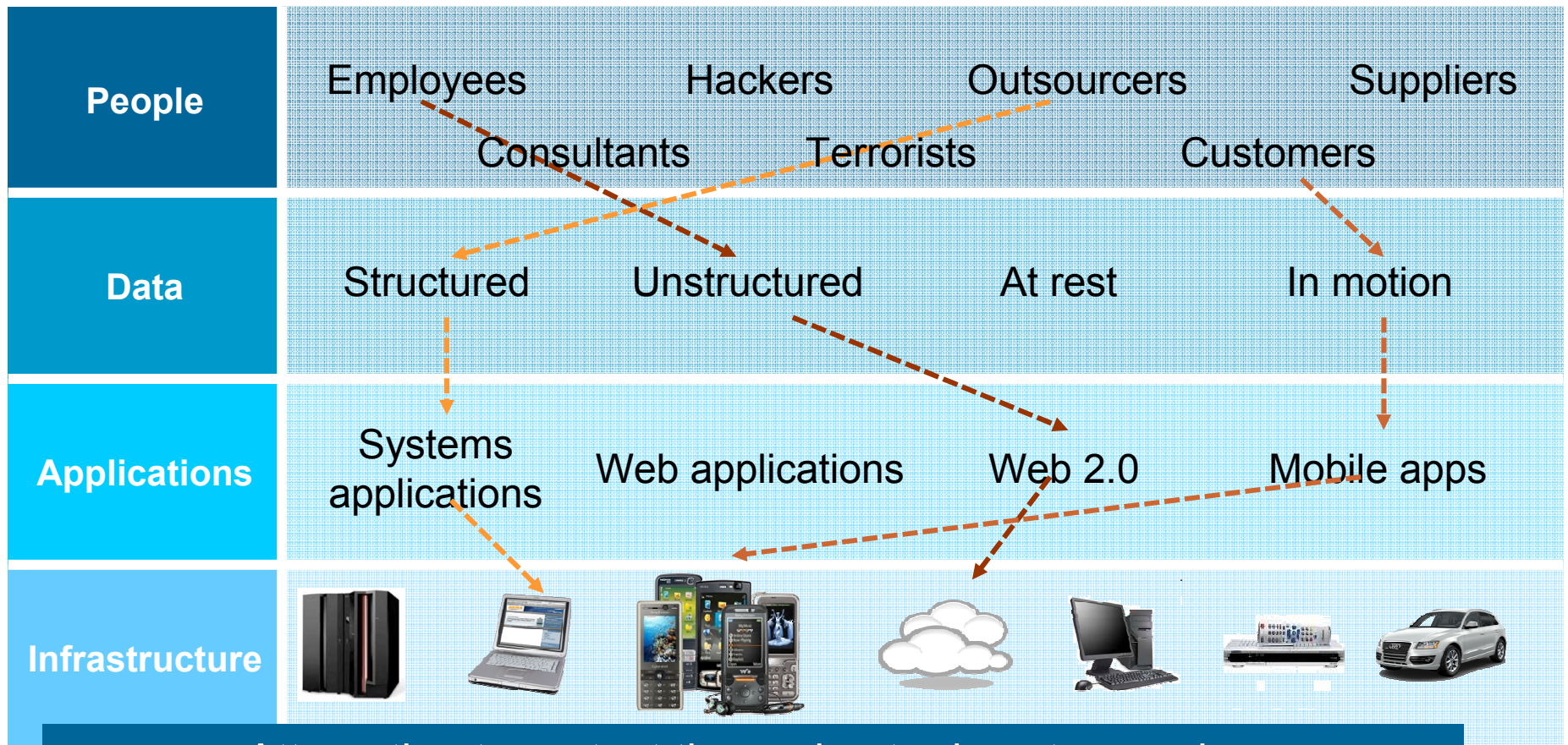
ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

IBMSecuritySymposium
Intelligence | Integration | Expertise

Solving a security issue is a complex, four-dimensional puzzle

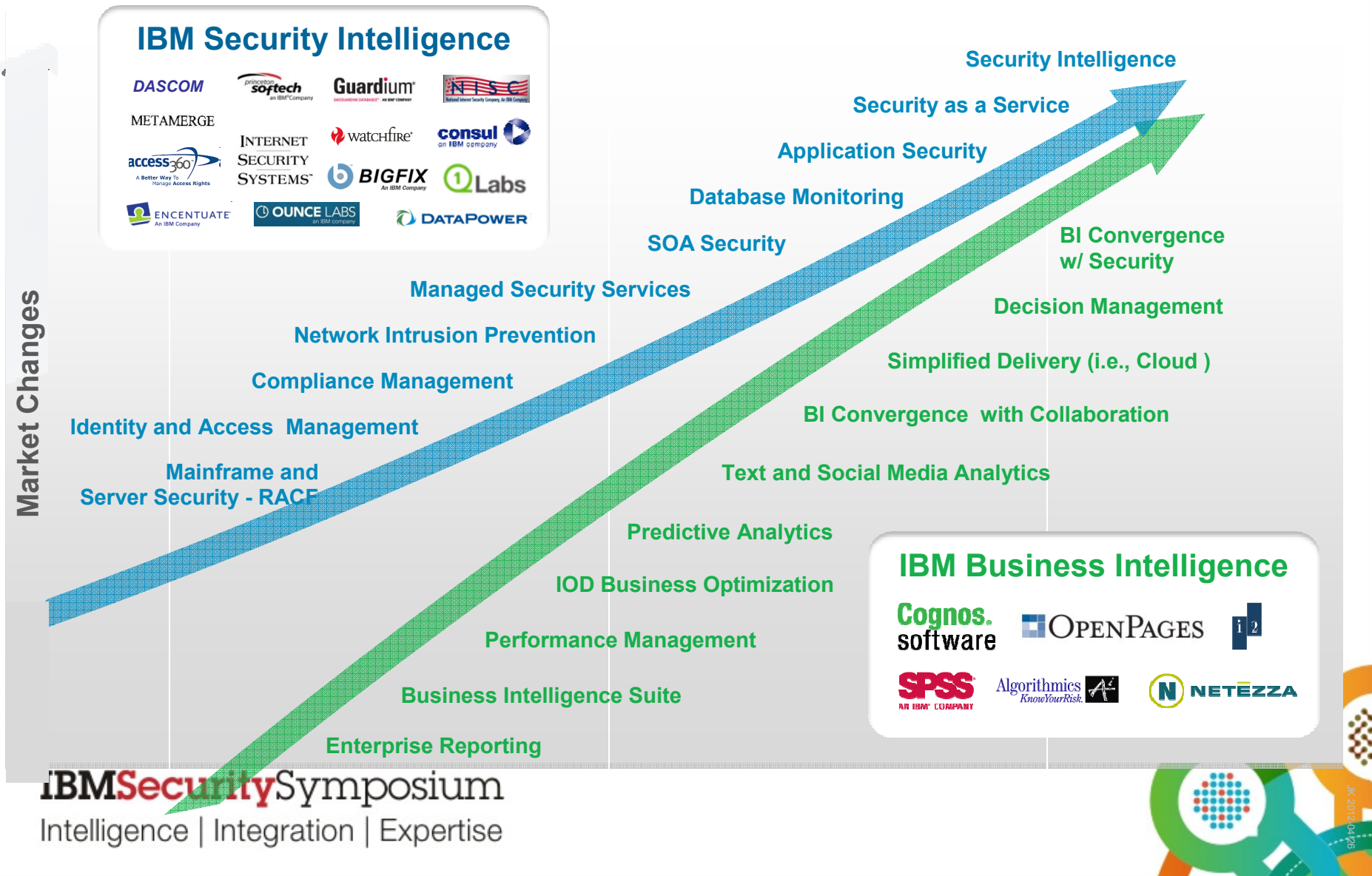|				
People	Employees	Hackers	Outsourcers	Suppliers
	Consultants	Terrorists		Customers
Data	Structured	Unstructured	At rest	In motion
Applications	Systems applications	Web applications	Web 2.0	Mobile apps
Infrastructure				

Attempting to protect the perimeter is not enough – siloed point products cannot adequately secure the enterprise

Security and Business Intelligence offer insightful parallels

Market Changes

IBM Security Intelligence

DASCOM | princeton softech an IBM Company | Guardium SAFEGUARDING DATABASES | NISC National Internet Security Company, An IBM Company

METAMERGE

access360 A Better Way To Manage Access Rights | INTERNET SECURITY SYSTEMS | watchfire | consul an IBM company

| BIGFIX An IBM Company | 1Labs

ENCENTUATE An IBM Company | OUNCE LABS an IBM company | DATAPOWER

Security Intelligence

Security as a Service

Application Security

Database Monitoring

SOA Security

Managed Security Services

Network Intrusion Prevention

Compliance Management

Identity and Access Management

Mainframe and Server Security - RACF

BI Convergence w/ Security

Decision Management

Simplified Delivery (i.e., Cloud)

BI Convergence with Collaboration

Text and Social Media Analytics

Predictive Analytics

IOD Business Optimization

Performance Management

Business Intelligence Suite

Enterprise Reporting

IBM Business Intelligence

Cognos software | OpenPages | i2

SPSS AN IBM COMPANY | Algorithmics KnowYourRisk. | NETEZZA

IBMSecuritySymposium
Intelligence | Integration | Expertise

Intelligence: Leadership in Coverage and Insight

	People	**Data**	**Applications**	**Infrastructure**
Security Intelligence	**Security Intelligence:** Information and event management Advanced correlation and deep analytics External threat research			
	Role based analytics Identity governance Privileged user controls	Data flow analytics Data governance	Secure app engineering processes Fraud detection	Advanced network monitoring Forensics / data mining Secure systems
Proficient	User provisioning Access mgmt Strong authentication	Access monitoring Data loss prevention	Application firewall Source code scanning	Virtualization security Asset mgmt Endpoint / network security management
Basic	Centralized directory	Encryption Access control	Application scanning	Perimeter security Anti-virus

Integration:

Increasing Security, Collapsing Silos, and Reducing Complexity

Increased Awareness and Accuracy

- Prevent advanced threats with real-time intelligence correlation across security domains
- Increase situational awareness by leveraging real-time feeds of X-Force Research and Global Threat Intelligence across IBM security products, such as QRadar SIEM and Network Security appliances
- Conduct complete incident investigations with unified identity, database, network and endpoint activity monitoring and log management

Ease of Management

- Simplify risk management and decision-making with automated reporting though a unified console
- Enhance auditing and access capabilities by sharing Identity context across multiple IBM security products
- Build automated, customized application protection policies by feeding AppScan results into IBM Network Intrusion Prevention Systems

Reduced Cost and Complexity

- Deliver fast deployment, increased value and lower TCO by working with a single strategic partner

Think Integrated.

People · Data · Applications · Network · Endpoint · Security Intelligence
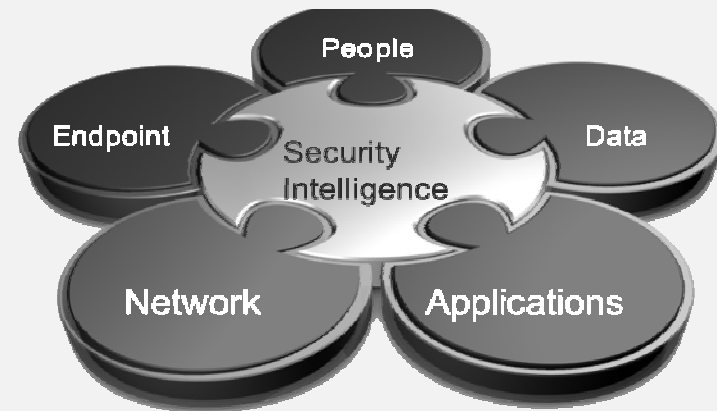
Expertise: Unmatched Global Coverage & Security Awareness

IBM

IBM Research

IBM Institute for Advanced Security

Enabling cybersecurity innovation and collaboration

Map locations:
Zurich, CH • IAS Americas • Delft, NL • IAS Europe • Ottawa, CA • Toronto, CA • Brussels, BE • Herzliya, IL • Boulder, US • TJ Watson, US • Almaden, US • Detroit, US • Tokyo, JP • Costa Mesa, US • Haifa, IL • Bangalore, IN • Tokyo, JP • Austin, US • Raleigh, US • Pune, IN • Taipei, TW • Atlanta, US • Bangalore, IN • Singapore, SG • Atlanta, US • Atlanta, US • Brisbane, AU • New Delhi, IN • Gold Coast, AU • Hortolândia, BR • Perth, AU • IAS Asia Pacific

WorldWide Managed
Security Services Coverage

- 20,000+ devices under contract
- 3,700+ MSS clients worldwide
- 9B+ events managed per day
- 1,000+ security patents*
- 133 monitored countries (MSS)

- 🟧 Security Operations Centers
- 🟢 Security Research Centers
- ⬜ Security Solution Development Centers
- 🏛 Institute for Advanced Security Branches

10B analyzed Web pages & images
150M intrusion attempts daily
40M spam & phishing attacks
46K documented vulnerabilities
Millions of unique malware samples

X FORCE

IBMSecuritySymposium
Intelligence | Integration | Expertise

IBM is integrating across IT silos with Security Intelligence solutions

Network Activity

Virtual Activity

Config/Change Info

Application Activity

Servers & Hosts

Security Systems

User Activity

Category

Credibility

Severity

Asset Discovery

Active Vulnerability Assessment

Passive Vulnerability Assessment

Statistical

Correlation

Rules Corelation

Attacker Profile

IP Location

Geo Location

User Logs

Network User

Application

Behavior

Activity Context

Offense ›

SUSPECTED INCIDENTS

IBMSecuritySymposium
Intelligence | Integration | Expertise

Key Recommendations

Trusting Identities

Managing Access

Securing Information

Protecting Data and Infrastructure

Valid Users?

Data at rest in databases and storage devices

Data in use by applications, OS and users

Data in motion

AUDIT & COMPLIANCE

Visibility – Know what data exists, what to protect, threats ..

Control – Network, Application, Data

IBMSecurity Symposium
Intelligence | Integration | Expertise

Automation - Change management process, patch management, …

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework
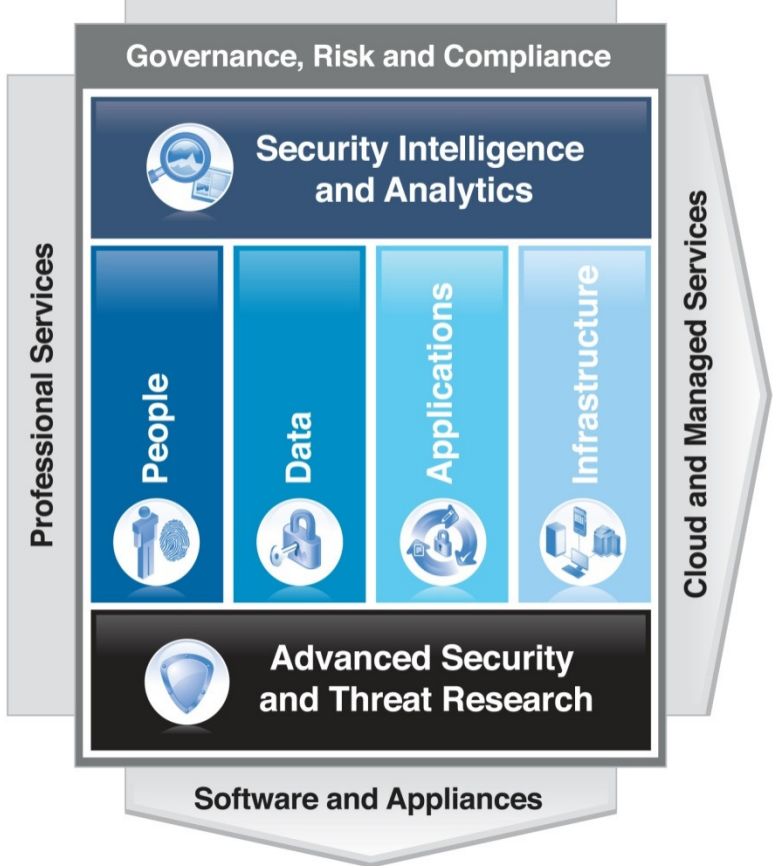

IBM Security Systems

- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • Integration • Expertise

IBM Security Framework

Governance, Risk and Compliance

Security Intelligence and Analytics

People | Data | Applications | Infrastructure

Advanced Security and Threat Research

Professional Services

Cloud and Managed Services

Software and Appliances

IBMSecurity**Symposium**
Intelligence | Integration | Expertise