Everyday Security:
Simple Solutions to Complex Security Problems

Sean Bergin

WW Sales Director, Tivoli Security
Welcome to the smart planet... and a smarter infrastructure

Globalization and Globally Available Resources

Billions of mobile devices accessing the Web

Access to streams of information in the Real Time

Dynamic Infrastructure

Improve Service: Reduce Cost: Manage Risk:

New Forms of Collaboration
Managing risks introduced by new opportunities

**Emerging technology**
- Virtualization and cloud computing increase infrastructure complexity.
- Web 2.0 and SOA style composite applications introduce new challenges with the applications being a vulnerable point for breaches and attack.

**Data and information explosion**
- Data volumes are doubling every 18 months.*
- Storage, security, and discovery around information context is becoming increasingly important.

**Wireless world**
- Mobile platforms are developing as new means of identification.
- Security technology is many years behind the security used to protect PCs.

**Supply chain**
- The chain is only as strong as the weakest link… partners need to shoulder their fair share of the load for compliance and the responsibility for failure.

**Clients expect privacy**
- An assumption or expectation now exists to integrate security into the infrastructure, processes and applications to maintain privacy.

**Compliance fatigue**
- Organizations are trying to maintain a balance between investing in both the security and compliance postures.

*Source: Pyramid Research, October 2007*
High-level cloud security concerns

**Loss of Control**
Many companies and governments are uncomfortable with the idea of their information located on systems they do not control. Providers must offer a high degree of security transparency to help put customers at ease.

**Data Security**
Migrating workloads to a shared network and compute infrastructure increases the potential for unauthorized exposure. Authentication and access technologies become increasingly important.

**Reliability**
High availability will be a key concern. IT departments will worry about a loss of service should outages occur. Mission critical applications may not run in the cloud without strong availability guarantees.

**Compliance**
Complying with SOX, HIPAA and other regulations may prohibit the use of clouds for some applications. Comprehensive auditing capabilities are essential.

**Security Management**
Providers must supply easy, visual controls to manage firewall and security settings for applications and runtime environments in the cloud.
Not all risks are created equal

Frequency of Occurrences Per Year

Data driven
- Virus
- Data Corruption
- Data Leakage
- Worms
- Disk Failure
- Application Outage
- System Availability Failures
- Network Problem

Business driven
- Lack of governance
- Failure to meet Industry standards
- Workplace inaccessibility
- Regional Power Failures
- Pandemic
- Building Fire

Event driven
- Terrorism/Civil Unrest
- Natural Disaster
- Failure to meet Compliance Mandates
- Pandemic
- Regional Power Failures
- Building Fire

Consequences (Single Occurrence Loss) in Dollars per Occurrence

$1 $10 $100 $1,000 $10k $100k $1M $10M $100M
How would you rate Security as a business priority?

Select the most appropriate answer

1. Our primary business focus is Control: access to data, applications & environments

2. Our business focus extends to Visibility: monitoring incidents and events

3. Our focus extends to include Compliance: audit and prove performance

4. Security Management is a key business directive and is given extreme focus from both an IT and an overall business perspective
Not all risk is created equally, neither are all security solutions…

- Find a balance between effective security and cost
  - The axiom… never spend $100 dollars on a fence to protect a $10 horse
- Studies show the Pareto Principle (the 80-20 rule) applies to IT security*
  - 87% of breaches were considered avoidable through reasonable controls
- Small set of security controls provide a disproportionately high amount of coverage
  - Critical controls address risk at every layer of the enterprise
  - Organizations that use security controls have significantly higher performance*

---

ITPI: IT Process Institute, EMA December 2008
IBM provides the business answers you need in uncertain times with solutions for all IT domains

Improving service, managing risk and reducing cost of Security without compromise

IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

- PEOPLE AND IDENTITY
- DATA AND INFORMATION
- APPLICATION AND PROCESS
- NETWORK, SERVER AND END POINT
- PHYSICAL INFRASTRUCTURE

IBM Service Management

Best Practices, Methodologies, and Services

Service Management Platform

Visibility | Control | Automation

Professional services | Managed services | Hardware and software
How would you rate Security as an IT priority?

Select the most appropriate answer

1. Our Security focus is primarily on Identity & Access Management
2. Our Security focus extends into Application Security
3. Our Security focus extends into securing information without negatively impacting service quality
4. We have an extensive Security program incorporated into our IT and business governance
IBM: The only security vendor in the market with end-to-end coverage of the security foundation

**Critical Security Processes**

**Manage Identities, Access and Entitlement:** Process for assuring access to enterprise resources has been given to the right people, at the right time, for the right purpose.

**Protect Data and Information:** Capability that allows for granular protection of unstructured & structured data, data leak prevention and acceptable use policy monitoring.

**Implement GRC Information and Event Management:** Log management capabilities designed to automate the process of auditing, monitoring and reporting on security and compliance posture across the enterprise.

**Address Threats and Vulnerabilities:** Process and capabilities designed to protect enterprise infrastructure from new and emerging threats.

**Assure Software and System Integrity:** Process for assuring efficiency and integrity of the software development & release lifecycle.

**Manage Assets:** Process for maintaining visibility and control over service and operational assets, and their impact on the business.

**Manage Change and Configuration:** Process for assuring routine, emergency and out-of-band changes are made efficiently, and in such a manner as to prevent operational outages.

**Manage Problems and Incidents:** Managed security operations center (SOC) or in-house Service Desk solutions designed to assure incidents are escalated and addressed in a timely manner. Forensics teams ready to respond to an emergency.
New Tivoli Security Solutions solve real customer challenges

<table>
<thead>
<tr>
<th>Identity and Access Assurance</th>
<th>Provide efficient and compliant access for right people to right resources at right time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data and Application Security</td>
<td>Protect integrity and confidentiality of business data and transactions from browser to disk</td>
</tr>
<tr>
<td>Security Management for z/OS</td>
<td>Secure and audit critical business services with your most trusted and resilient platform</td>
</tr>
</tbody>
</table>
### Issues

- Increasing number of industry and regulatory requirements
- Reputational and financial risks of non-compliance
- Cost of preparing for audits and assessments
- Difficulty determining and documenting effectiveness of controls
- Internal policy violations
- Audit findings

### Select IBM Security Offerings

- **Audit Readiness Workshops and Assessments:** Security Health check, Security Workshop, Security Risk Assessment, Compliance Assessments
- **Controls Effectiveness Assessments:** Penetration Testing, Regulation-specific Assessments
- **Controls and Governance Services:** IBM ISS Governance Services for compliance and regulatory services, Information Security Framework
- **Compliance Management and Reporting:** Tivoli Compliance Insight Manager, Tivoli zSecure Audit, IBM Compliance Warehouse, IBM Records Manager

### Values

- Demonstrable policy enforcement aligned to regulations, standards, laws, agreements
- Decreases reputational risk and penalties and fines for non-compliance
- Enables cost effective audit and assessment preparation by automating reporting and documentation efforts
- Provides visibility into controls effectiveness and policy violations, reducing risk of internal and external threats
- Improves security posture to reduce audit findings
Which best describes your current Identity & Access Management capability?

Select the most appropriate answer

1. Users sign on to individual applications, minimal infrastructure exists for security monitoring and auditing.

2. Multiple user registries and access control policies are defined in multiple places.

3. A consistent practice and a consistent infrastructure for access control are implemented. Provisioning of account information is policy-based and consistently applied.

4. Identity and access management are tied to the employee life cycle in the organization. Automated policy-based administration of users' accounts streamlines administration across the organization.
## People and Identity

### Issues
- Understanding the identity risk gap
- Cost of administering users and identities in-house
- Privileged user activity unmonitored
- Dormant IDs or shared identities being used to inappropriately access resources
- Failing an audit

### Select IBM Security Offerings
- **Identity Lifecycle Management**: Tivoli Identity and Access Management solution, Tivoli Security Management for z/OS solution
- **High-Assurance Digital Identities**: Trusted Identity Initiative
- **Identity Audit**: Tivoli Compliance Insight Manager, Tivoli zSecure Audit
- **Identity Services**: Identity & Access Design and Implementation Services, ISS Managed Identity Services, Identity Risk and Investigation Solution (IRIS) and

### Values
- Reduces the cost, increases efficiency and enables audit-ability of managing flow of users entering, using, and leaving the organization
- Decreases risk of internal fraud, data leak, or operational outage
- Supports globalization of operations
- Enables shift from traditional brick & mortar sales to delivery of on-line services to customers and partners across the globe
- Improves end-user experience with Web-based business applications by enabling such activities such as single sign-on

Manage Identities and Access

“How can my business benefit from management of digital identity?”

IBM Insight Forum 09
Data and Information

**Issues**

- Data stored on removable media that can be lost/stolen
- Data stored in the clear is easily accessible
- Inconsistent data policies
- Unstructured and/or unencrypted data
- Legal, regulatory and ethical exposure for the organization
- Costs of data breaches, notification, brand value
- Failing an audit

**Select IBM Security Offerings**

- **Data Loss Prevention**: ISS Data Security and Data Loss Prevention solution
- **Protecting Data at Rest or In Transit**: Tivoli Application and Data Security solution, WebSphere MQ Extended Security Edition, WebSphere DataPower Appliances
- **SIEM**: Tivoli Compliance Insight Manager, ISS SiteProtector
- **Data Encryption**: Tivoli Key Lifecycle Manager, encrypted tape and disk drives
- **Data Classification**: InfoSphere Information Analyzer, Cognos, Enterprise Content Management, Discovery and Classification, IBM Records Manager
- **Unstructured Data Security**: Tivoli Access Manager
- **Data Confidentiality**: Optim Data Privacy solution, Lotus Protector for Mail Security
- **Security Services**: ISS Professional and Managed Security Services, Security Event and Log Management Services

**Values**

- Reduces the cost, increases ability to meet audit and compliance mandates
- Provides a cost-effective way to meet legal discovery, hold and retention requirements
- Assures data is available to the right people, at the right time
- Assures data is not deliberately or inadvertently taken, leaked, or damaged
- Decreases number and complexity of controls integrated within the enterprise
## Issues

<table>
<thead>
<tr>
<th>Application and Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web applications #1 target of hackers seeking to exploit vulnerabilities</td>
</tr>
<tr>
<td>Increasing number of attacks via XML scripting and virus insertion</td>
</tr>
<tr>
<td>Applications are deployed with vulnerabilities</td>
</tr>
<tr>
<td>Poor security configs expose clients to business loss</td>
</tr>
<tr>
<td>PCI regulatory requirements mandate application security</td>
</tr>
<tr>
<td>80% of development costs spent on identifying and fixing defects</td>
</tr>
<tr>
<td>Real and/or private data exposed to anyone with access to development and test environments, including contractors and outsourcers</td>
</tr>
</tbody>
</table>

## Select IBM Security Offerings

<table>
<thead>
<tr>
<th>Application Security</th>
<th>Application Controls</th>
<th>Messaging Security</th>
<th>Security for SOA</th>
<th>Application Security Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rational AppScan, Rational AppScan Malware Scanning, IBM Web Application Module WebSphere DataPower Appliances</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tivoli Access Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WebSphere DataPower, Tivoli Security Policy Manager, Tivoli Federated Identity Manager, WebSphere Services Registry &amp; Repository</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ISS Application Security Risk Assessment Services, ISS Managed Security Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Values

<table>
<thead>
<tr>
<th>Secure Web Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;How can my business benefit from management of application security?&quot;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce risk of outage, defacement or data theft associated with web applications</td>
</tr>
<tr>
<td>Assess and monitor enterprise-wide security policy compliance</td>
</tr>
<tr>
<td>Improve compliance with industry standards and regulatory requirements (e.g., PCI, GLBA, HIPAA, FISMA, etc.)</td>
</tr>
<tr>
<td>Improve ability to integrate business critical applications securely</td>
</tr>
<tr>
<td>Automated testing and governance throughout the development lifecycle, reducing long-term security costs</td>
</tr>
<tr>
<td>Issues</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>▪ Parasitic, stealthier, more damaging attacks</td>
</tr>
<tr>
<td>▪ Poor understanding of risks in new technologies and applications, including virtualization and cloud</td>
</tr>
<tr>
<td>▪ Weak application controls</td>
</tr>
<tr>
<td>▪ Lack of skills to monitor and manage security inputs</td>
</tr>
<tr>
<td>▪ Compounding cost of managing an ever increasing array of security technologies</td>
</tr>
<tr>
<td>▪ Undetected breaches due to privilege access misuse and downtime from incidents</td>
</tr>
<tr>
<td>▪ Inability to establish forensic evidence or demonstrate compliance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ Reduces cost of ongoing management of security operations</td>
</tr>
<tr>
<td>▪ Improves operational availability and assures performance against SLA, backed by industry’s only guaranteed SLA for managed protection services</td>
</tr>
<tr>
<td>▪ Increases productivity by decreasing risk of virus, worm and malcode infestation</td>
</tr>
<tr>
<td>▪ Decreases volume of incoming spam</td>
</tr>
<tr>
<td>▪ Drill down on specific violations to quickly address resolution</td>
</tr>
<tr>
<td>▪ Readily show status against major regulations</td>
</tr>
</tbody>
</table>
IBM professional security services

Proven integrated lifecycle methodology that delivers ongoing security solutions

Phase 5: Education
- IBM ISS Product Courses
  - On-site & off-site classes

Phase 4: Management and Support
- Staff Augmentation
- Emergency Response Service

Phase 3: Deployment
- Implementation and Optimization
- Migration Services

Phase 2: Design
- Policy Development
- Incident Response Planning
- Standards and Procedures Development
- Implementation Planning

Phase 1: Assessment
- Threat Mitigation
- Governance Risk and Compliance
- Data Security
- Identity & Access
- Physical Security
- Application Security
Analysts Recognize IBM Security Leadership

- **Gartner Leadership**
  - Security Information & Event Management Magic Quadrant (May 2009)
  - Web Access Management Magic Quadrant (November 2008)
  - User Provisioning Magic Quadrant (August 2008)
  - Master Data Management for Customer Data Magic Quadrant (July 2008)
  - Managed & Professional Network Service Providers, North America Magic Quadrant (May 2008)
  - Business Intelligence and Performance Management Services, North America Magic Quadrant (May 2008)
  - Managed Security Service Providers, APAC Marketscope – Strong Positive (May 2008)
  - Managed Security Service Providers, Europe Marketscope - Strong Positive (May 2008)
  - FilesX – Cool Vendors in Data Protection (March 2008)
  - Network Intrusion Prevention System Appliances Magic Quadrant (February 2008)
  - Managed Security Services Providers, North America Magic Quadrant (August 2007)

- **Forrester Leadership**
  - Managed Security Services Wave (October 2007)
  - Risk Consulting Services Wave (June 2007)

- **IDC Market Share Leadership**
  - #1 Identity & Access Management (2008)
  - #1 Identity Management Provider (2007)
  - #1 Vulnerability Assessment Software Worldwide (2007)
  - #1 Application Vulnerability Assessment Software Worldwide (2007)

- **Frost & Sullivan Leadership**
  - IDS/IPS Market Leader (2007)
Tivoli is established leader in IAM and SIEM markets

- #1 Identity and Access Management Market Share (IDC) – past 3 years
- #1 SIEM Market Share (Gartner)
- Over 2,700 customers worldwide
IBM: Comprehensive Security Risk & Compliance Management

- The only security vendor in the market with end-to-end coverage of the security foundation
- 15,000 researchers, developers and SMEs on security initiatives
- 3,000+ security & risk management patents
- 200+ security customer references and 50+ published case studies
- 40+ years of proven success securing the mainframe environment
Thank you

Questions?