IBM Security, Risk and Compliance Management Roadmap
2010

Presented by:
Joe Hamblin CISSP
IBM Chief Federal Cyber Security Specialist
Introducing IBM Security Solutions

The planet is getting more
Instrumented, Interconnected and Intelligent.

New possibilities.
New risks...

Is the smarter planet secure?
Pervasive instrumentation creates vast amounts of data

New services built using that data, raises
Privacy and Security concerns...

Critical physical and IT infrastructure
Sensitive information protection
New denial of service attacks
Increasing risks of fraud
The IBM Security Framework foundation addresses your challenges of cost, complexity and compliance

Build a strong foundation for IT security

Create and sustain security governance

Manage risk

Ensure compliance
In addition to the foundational elements, the Framework identifies five security focus areas as starting points:

- **GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE**: Design, and deploy a strong foundation for security & privacy.
- **PEOPLE AND IDENTITY**: Mitigate the risks associated with user access to corporate resources.
- **DATA AND INFORMATION**: Understand, deploy, and properly test controls for access to and usage of sensitive data.
- **APPLICATION AND PROCESS**: Keep applications secure, protected from malicious or fraudulent use, and hardened against failure.
- **NETWORK, SERVER AND END POINT**: Optimize service availability by mitigating risks to network components.
- **PHYSICAL INFRASTRUCTURE**: Provide actionable intelligence on the desired state of physical infrastructure security and make improvements.
IBM Security portfolio can help you meet challenges in each security focus area

<table>
<thead>
<tr>
<th>Framework</th>
<th>Typical enterprise activities</th>
<th>GRC</th>
</tr>
</thead>
<tbody>
<tr>
<td>GOVERNANCE, RISK MGMT, COMPLIANCE</td>
<td>- Security Strategy Design</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Pen Testing &amp; Vulnerability Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Security Compliance Assessment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Incident Response</td>
<td>GRC</td>
</tr>
<tr>
<td>PEOPLE AND IDENTITY</td>
<td>- Manage identities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Control access to applications</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Audit, report and manage access to resources</td>
<td></td>
</tr>
<tr>
<td>DATA AND INFORMATION</td>
<td>- Protect Critical Databases</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Messaging Security and Content Filtering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Monitor &amp; manage data access</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Prevent Data Loss</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Encrypt sensitive data</td>
<td></td>
</tr>
<tr>
<td>APPLICATION AND PROCESS</td>
<td>- Ensure Security in App Development</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Discover App Vulnerabilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Embed App Access Controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Provide SOA Security</td>
<td></td>
</tr>
<tr>
<td>NETWORK, SERVERS &amp; ENDPOINTS</td>
<td>- Protect Servers, Endpoints, Networks, Mainframes</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Provide Video Surveillance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Establish Command and Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Capture video analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Manage security across all assets</td>
<td></td>
</tr>
<tr>
<td>PHYSICAL INFRASTRUCTURE</td>
<td>- Provide Video Surveillance</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Establish Command and Control</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Capture video analytics</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Manage security across all assets</td>
<td></td>
</tr>
</tbody>
</table>

Click for more information

© 2010 IBM Corporation
Introducing IBM Security Solutions

**Is the smarter planet secure?**

The planet is getting more
Instrumented, Interconnected and Intelligent.

**New possibilities.**

**New risks...**

Pervasive instrumentation creates vast amounts of data

New services built using that data, raises
Privacy and Security concerns...

- Critical physical and IT infrastructure
- Sensitive information protection
- New denial of service attacks
- Increasing risks of fraud
Security challenges in a smarter planet

Key drivers for security projects

- **Increasing Complexity**
  
  Soon, there will be 1 trillion connected devices in the world, constituting an “internet of things”

- **Rising Costs**
  
  Spending by U.S. companies on governance, risk and compliance will grow to $29.8 billion in 2010

- **Ensuring Compliance**
  
  The cost of a data breach increased to $204 per compromised customer record

Source
Cost, complexity and compliance

Emerging technology

Data and information explosion

Death by point products

Rising Costs: Do more with less

Compliance fatigue

People are becoming more and more reliant on security

IBM believes that security is progressively viewed as every individual’s right
## BUSINESS VALUE

Ensure comprehensive management of security activities and compliance with all security mandates

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Design and implement secure deployment strategies for advanced technologies such as Cloud, virtualization, etc.</td>
<td>Identify and eliminate security threats that enable attacks against systems, applications and devices</td>
<td>Perform security compliance assessments against PCI, ISO and other standards and regulations</td>
<td>Design and implement policy and processes for security governance, incident response; perform timely response and computer forensics</td>
<td></td>
</tr>
</tbody>
</table>

| Software | Rational® AppScan®; Guardium Database Monitoring & Protection | Tivoli Security Information and Event Manager; Guardium Database Monitoring & Protection; Tivoli zSecure suite | Tivoli® Security Information and Event Manager; Tivoli zSecure suite |

This is not intended to be a comprehensive list of all IBM products and services
## BUSINESS VALUE

Lower costs and mitigate the risks associated with managing user access to corporate resources

<table>
<thead>
<tr>
<th>Business Challenge</th>
<th>Cost and Complexity of Managing Identities</th>
<th>Providing Access to Applications</th>
<th>Auditing, reporting and managing access to resources</th>
</tr>
</thead>
</table>
|                    | ▪ On average, enterprises spend 2 weeks to setup new users on all systems and about 40% of accounts are invalid  
                            ▪ 30% of help desk calls are for password resets, at $20 per call | “We would need to spend $60k on each of our 400 applications to implement security access rules”  
                                                                                       – Global financial services firm | ▪ Privileged users cause 87% of internal security incidents, while firms cannot effectively monitor thousands of security events generated each day  
                                                                                       ▪ Role management, recertification, etc. |
| Software           | Tivoli® Identity and Access Assurance, Tivoli zSecure suite | Tivoli Access Manager, Tivoli Federated Identity Manager | Tivoli Identity Manager and Access Assurance, Tivoli Security Information and Event Manager |

This is not intended to be a comprehensive list of all IBM products and services
IBM Security Solutions

Identity and Access
- Identity Manager
- Access Manager for e-business
- Access Manager for Enterprise SSO
- Federated Identity Manager
- Directory Server
- Directory Integrator
- Security Policy Manager
- Privileged Identity Manager
- zSecure suite

Data and Application Security
- Security Policy Manager
- Security Web Gateway
- Information Loss Protection
- Key LifeCycle Manager
- Deep Content Analysis SDK
- Multifunction Security

Data Center And Operational Security
- Security Server Protection
- Security SiteProtector System
- Virtual Server Protection
- RealSecure Server Sensor
- Network Intrusion Prevention Appliances
- Network Intrusion Prevention Virtual Appliance
- Enterprise Scanner
- Desktop Security
Implementing identity and access management can address these challenges and drive positive results

- Can reduce the time to onboard and de-provision identities from weeks to minutes
- Can significantly reduce help desk costs resulting from password reset calls
- Decreases risk of internal fraud, data leak, or operational outage
- Improves end-user experience with Web-based business applications by enabling such activities such as single sign-on
The challenges of managing digital identities

- Dormant IDs or shared identities being used to inappropriately access resources
- Cost of administering users and identities in-house
- Privileged user activity unmonitored
- Meeting compliance requirements, responding to audits
### BUSINESS VALUE

**Understand, deploy and properly test controls for access to and usage of sensitive business data**

<table>
<thead>
<tr>
<th>Business Challenge</th>
<th>Protecting Critical Databases</th>
<th>Messaging Security and Content Filtering</th>
<th>Managing Data Access and Encryption</th>
<th>Monitoring Data Access and Preventing Data Loss</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Mitigate threats against databases from external attacks and internal privileged users</td>
<td>Spam and inappropriate Web sites pose major productivity drains, resource capacity strains, and leading attack vector for malware</td>
<td>Over 82% of firms have had more than one data breach in the past year involving loss or theft of 1,000+ records with personal information; cost of a data breach increased to $204 per compromised customer record*</td>
<td>42% of all cases involved third-party mistakes and flubs… magnitude of breach events ranged from about 5,000 to 101,000 lost or stolen customer records*</td>
</tr>
</tbody>
</table>

| Software            | Guardium Database Monitoring & Protection | Multi-Function Security appliance, Lotus Protector | Tivoli® Key Lifecycle Manager, Tivoli Security Policy Manager, Tivoli Federated Identity Manager | Data Loss Prevention; Tivoli Security Information and Event Manager |

* *Fifth Annual U.S. Cost of Data Breach Study*, Ponemon Institute, Jan 2010
## Business Challenge

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Vulnerabilities caught early in the development process are orders of magnitude cheaper to fix versus after the application is released.</td>
<td>▪ 74% of vulnerabilities in applications have no patch available today*&lt;br&gt;▪ 80% of development costs are spent identifying and correcting defects, costing $25 during coding phase vs. $16,000 in post-production**</td>
<td>According to customers, up to 20% of their application development costs can be for coding custom access controls and their corresponding infrastructure.</td>
<td>Establishing trust and high performance for services that span corporate boundaries is a top priority for SOA-based deployments.</td>
<td></td>
</tr>
</tbody>
</table>

| Software | Rational® AppScan®; Ounce | Rational AppScan; Ounce | Tivoli® Identity and Access Assurance | WebSphere® DataPower®; Tivoli Security Policy Manager |

---

* IBM X-Force Annual Report, Feb 2009  
** Applied Software Measurement, Caper Jones, 1996  
This is not intended to be a comprehensive list of all IBM products and services
IBM Security Solutions

Identity and Access

- Identity Manager
- Access Manager for e-business
- Access Manager for Enterprise SSO
- Federated Identity Manager
- Directory Server
- Directory Integrator
- Security Policy Manager
- Privileged Identity Manager
- zSecure suite

Data and Application Security

- Security Policy Manager
- Security Web Gateway
- Information Loss Protection
- Key LifeCycle Manager
- Deep Content Analysis SDK
- Multifunction Security

Data Center and Operational Security

- Security Server Protection
- Security SiteProtector System
- Virtual Server Protection
- RealSecure Server Sensor
- Network Intrusion Prevention Appliances
- Network Intrusion Prevention Virtual Appliance
- Enterprise Scanner
- Desktop Security

IBM Confidential
## BUSINESS VALUE

Optimize service availability by mitigating risks while optimizing expertise, technology and process

### Business Challenge

<table>
<thead>
<tr>
<th>Protecting Servers</th>
<th>Protecting Endpoints</th>
<th>Protecting Networks</th>
<th>Protecting Mainframes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mitigate threats against servers; prevent data loss</strong></td>
<td><strong>Effective management can cut total cost of ownership for secured desktops by 42%</strong>&lt;sup&gt;*&lt;/sup&gt;</td>
<td><strong>Mitigate network based threats and prevent data loss</strong></td>
<td><strong>Mitigate threats against mainframes; protect against vulnerabilities from configuration; contain the privileged users</strong></td>
</tr>
</tbody>
</table>

**Software**

<table>
<thead>
<tr>
<th>Protecting Servers</th>
<th>Protecting Endpoints</th>
<th>Protecting Networks</th>
<th>Protecting Mainframes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Protection, Server Protection for VMWare</td>
<td>Desktop security platform; encryption</td>
<td>Network Intrusion Prevention System (IPS)</td>
<td>Tivoli® zSecure suite</td>
</tr>
</tbody>
</table>

<sup>*</sup> Gartner Desktop Total Cost of Ownership: 2008 Update, Jan 2008

This is not intended to be a comprehensive list of all IBM products and services
IBM Security Solutions

Identity and Access
- Identity Manager
- Access Manager for e-business
- Access Manager for Enterprise SSO
- Federated Identity Manager
- Directory Server
- Directory Integrator
- Security Policy Manager
- Privileged Identity Manager
- zSecure suite

Data and Application Security
- Security Policy Manager
- Security Web Gateway
- Information Loss Protection
- Key LifeCycle Manager
- Deep Content Analysis SDK
- Multifunction Security

Data Center And Operational Security
- Security Server Protection
- Security SiteProtector System
- Virtual Server Protection
- RealSecure Server Sensor
- Network Intrusion Prevention Appliances
- Network Intrusion Prevention Virtual Appliance
- Enterprise Scanner
- Desktop Security
### Physical infrastructure

#### BUSINESS VALUE

Provide actionable intelligence and improve effectiveness of physical infrastructure security

<table>
<thead>
<tr>
<th>Business challenge</th>
<th>Video Surveillance</th>
<th>Video Analytics</th>
<th>Command and Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legacy analog video systems with proprietary interfaces are hard to integrate with IT infrastructure</td>
<td>Video information from many cameras present an information overload to human security personnel, detection is often after the fact and response management is problematic</td>
<td>IT and physical security operate in silos and do not integrate. It is increasingly difficult and expensive to consolidate security information across locations for effectiveness and compliance</td>
<td></td>
</tr>
<tr>
<td>IT infrastructure, Logical Security products, and DVS partner products</td>
<td>Smart Vision Suite</td>
<td>Command Control Center Solution</td>
<td></td>
</tr>
</tbody>
</table>

This is not intended to be a comprehensive list of all IBM products and services
Three reasons why virtualization infrastructure protection is important

<table>
<thead>
<tr>
<th>Need</th>
<th>How IBM Security Virtual Server Protection for VMware® helps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mitigate new risks and complexities introduced by Virtualization</td>
<td>Provides dynamic protection for every layer of the virtual infrastructure</td>
</tr>
<tr>
<td>Maintain compliance standards and regulations</td>
<td>Helps meet regulatory compliance by providing security and reporting functionality customized for the virtual infrastructure</td>
</tr>
<tr>
<td>Drive operational efficiency</td>
<td>Increases ROI of the virtual infrastructure</td>
</tr>
</tbody>
</table>
Why IBM?
IBM’s research makes us a visionary in the future of IT Security

Building the technology of tomorrow

**Homomorphic Encryption**
Query a search engine without telling the engine what you are looking for!

**Enterprise Security Architecture**
Working with clients worldwide to implement the new architecture based on six security zones of control

**High Tech Risk Analytics**
Pre-fraud detectors with low false positive rates at a speed of 15-20 times the scale of today's model

Source: [https://www.privacyassociation.org/about_iapp/2009_09_17_iapp_honors_top_privacy_innovators](https://www.privacyassociation.org/about_iapp/2009_09_17_iapp_honors_top_privacy_innovators)
Thank You
Identity and Access

**Strategy:**

Increase the value that customers realize by extending the identity context to application, data, and threat management.

**Drivers:**

- Simplification
- Compliance
- Virtualization
- Application & Data Protection

**Innovation/Integration Focus Areas:**

- **Expand IAM Governance Capabilities:** Deliver role discovery and mining product to complement the existing operational role management capabilities, while continuing to support a services based Privileged Identity Management offering.

- **Decreased operational costs:** Improved integration between key products, and targeted operational improvements to improve ROI based on customer feedback.

- **Enterprise Security Hub:** Expand the number of mainframe products that zSecure supports and enable the expansion of Linux on System z to secure the organization’s datacenter.
Data and Application Security

Strategy:
Deliver innovative, integrated new solutions to address critical compliance and data protection challenges

Innovation/Integration Focus Areas:

Data Loss Prevention and Content Aware Access Control
- FileNet and DB2 entitlement management in Beta (TSPM)
- Identify PII leakage as part of complete network protection (IPS)
- Endpoint discovery and control over sensitive data (future)

Application Security / Content Control (Security Web Gateway)
- Expand access control to external Web content/apps (Future)
- Protect Web Apps against attack/malware

End-to-End Compliance Visibility
- Insider threat/compliance monitoring across Data and App Security
- Integration with FIM, TSPM, TKLM, & IPS. Guardium in roadmap

Standards Leadership
- Driving XACML through J2EE,.NET, and data services via TSPM
- Leadership in encryption key management standard (KMIP)

Drivers:

- Simplification
- Compliance
- Cloud / Web 2.0
- Data & Application Protection
Data Center and Operational Security

Strategy:

Address the security and compliance requirements to manage threats against the data center and enterprises adopting virtualization and cloud.

Drivers:

Innovation/Integration Focus Areas:

Virtual Server Protection
- Increase the capabilities, performance, and platforms supported by virtual server and physical security product lines.
- Further integrate within IBM’s offerings for applications, server farms, cloud computing and datacenters.

Network Intrusion Prevention
- Move beyond traditional IPS feature set and deliver high performance and increased security capabilities leveraging IBM processor expertise.
- Expand feature capabilities of IPS appliance to address the needs of customers whose primary mission is to secure the organization’s datacenter.

Endpoint (Server) Intrusion Prevention
- Integration of Endpoint Protection, Single Sign On, Tivoli Endpoint Management, to address compliance and threat.
- Use Virtual Server Protection to address threat protection in virtualized environments (hypervisor) while using an integrated Tivoli/ISS server agent to address compliance needs within the virtualized or physical servers.

Drivers:

Simplification
Compliance
Cloud / Web 2.0
Threat Protection