Pulse
Comes to You 2009

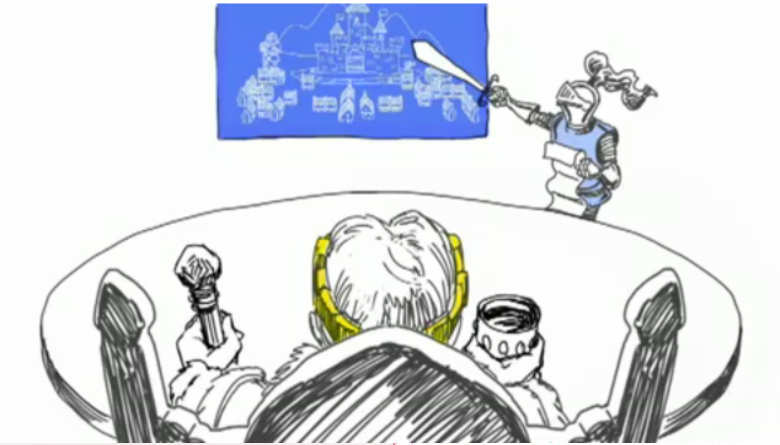
IBM

Managing the World's Infrastructure

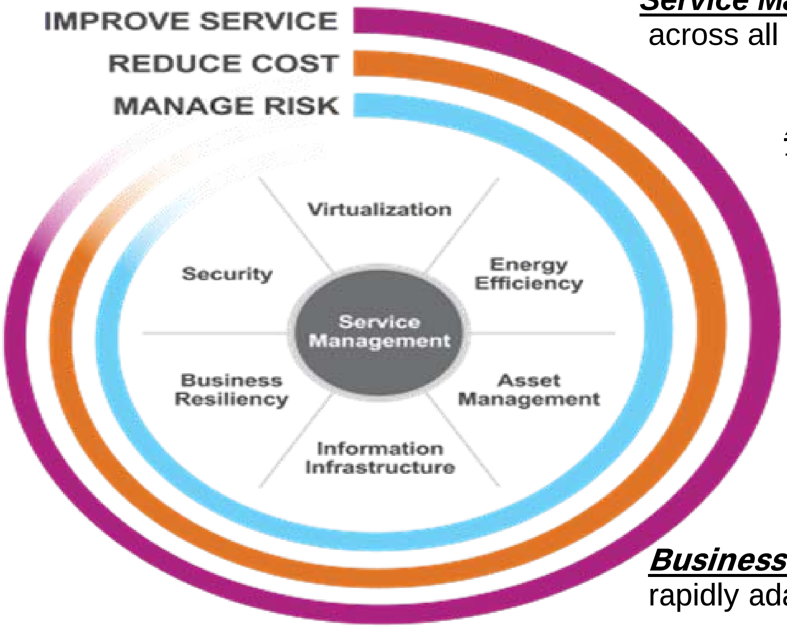
IBM Security Framework & Tivoli Security, Risk and Compliance Update

Peter Jopling

The King, the Dragon and the Secure Cloud



Building a dynamic infrastructure



Service Management – Provide visibility, control and automation across all the business and IT assets to deliver higher value services.

Asset Management – Maximizing the value of critical business and IT assets over their lifecycle with industry tailored asset management solutions.

Energy Efficiency – Address energy, environment, and sustainability challenges and opportunities across your infrastructure.

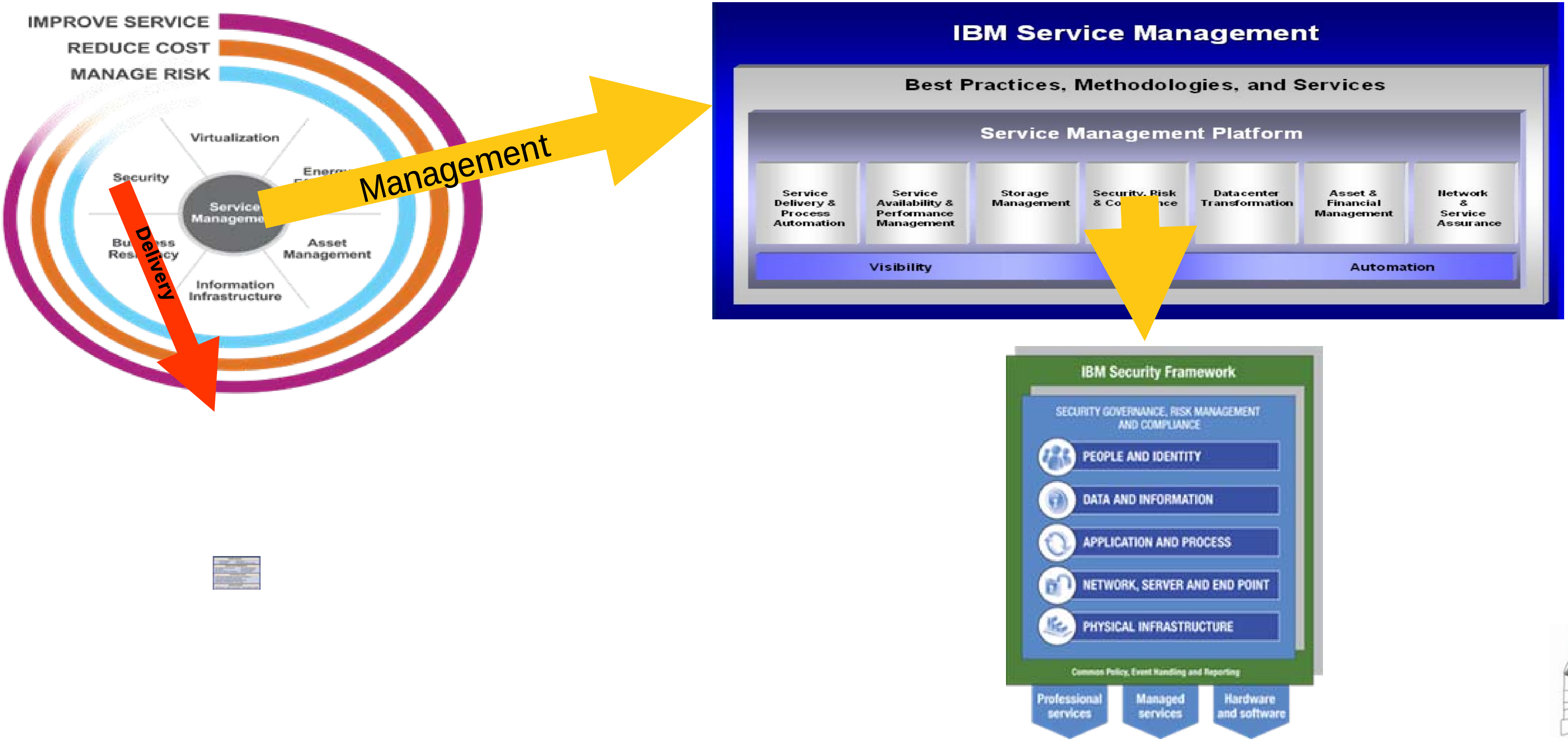
Virtualization – Leadership virtualization and consolidation solutions that reduce cost, improve asset utilization, and speed provisioning of new services.

Business Resiliency – Maintaining continuous business operations while rapidly adapting and responding to risks and opportunities.

Security End to end industry customized governance, risk management and compliance solutions.

Information Infrastructure – Helping businesses achieve information compliance, availability, retention, and security objectives.

Delivering & Managing a Secure dynamic infrastructure.



IMPROVE SERVICE

REDUCE COST

MANAGE RISK

Virtualization

Energy Efficiency

Security

Service Management

Business Resiliency

Asset Management

Information Infrastructure

Delivery

Management

IBM Service Management

Best Practices, Methodologies, and Services

Service Management Platform

Service Delivery & Process Automation	Service Availability & Performance Management	Storage Management	Security, Risk & Compliance	Datacenter Transformation	Asset & Financial Management	Network & Service Assurance

Visibility

Automation

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

Common Policy, Event Handling and Reporting

Professional services | Managed services | Hardware and software

Governance

Privacy

Threat mitigation

Transaction and data integrity

Identity and access management

Application security

Physical security

Personnel security

Governance

Strategy
- Information security policy
- Enterprise security architecture

Governance framework
- Governance structure

Information security advisory
- Consulting and advisory services

Security risk management framework
- Threat risk assessment
- Information asset profile
- Project risk assessment
- Security risk management

Compliance program
- Regulatory compliance
- Technical, policy and standards compliance
- Health checking
- Internal audit and response

Privacy

Privacy and information management strategy
- Define privacy information strategy
- Requirements and compliance process
- Incident response

Policy, practices and controls
- Policy taxonomy and glossary
- Policy rules definitions
- Privacy impact assessment (proactive)
- Privacy audit (reactive)
- Awareness and training

Data, rules and objects
- Privacy data taxonomy and classification
- Privacy business process model
- Data usage compliance process

Threat mitigation

Network segmentation and boundary protection
- Network zone management and boundary security infrastructure
- Remote access infrastructure
- Intrusion defense
- Network security infrastructure

Content checking
- Virus protection
- Content filtering

Vulnerability management
- Standard operating environment
- Patch management
- Vulnerability scanning and assessment

Incident management
- Incident management
- Event correlation
- Forensics

Transaction and data integrity

Business process transaction security
- Fraud detection
- Data transaction security

Database security
- Database configuration
- Master data control

Message protection
- Public key infrastructure
- Message protection security

Secure storage
- Data retrieval
- Data storage protection
- Data destruction
- Archiving

Systems integrity
- Security in systems management
- Security in business continuity planning

Identity and access management

Identity proofing
- Access management
- Background screening
- Identity establishment

Access management
- Single sign-on
- Authentication services
- Access control services

Identity lifecycle management
- User provisioning
- Other entity provisioning
- Identity credential management

Application security

Systems development lifecycle (SDLC)
- Security in the SDLC process

Application development environment
- Secure coding practices
- Operational application support environment
- Design patterns

Physical security

Site security
- Site planning
- Site management

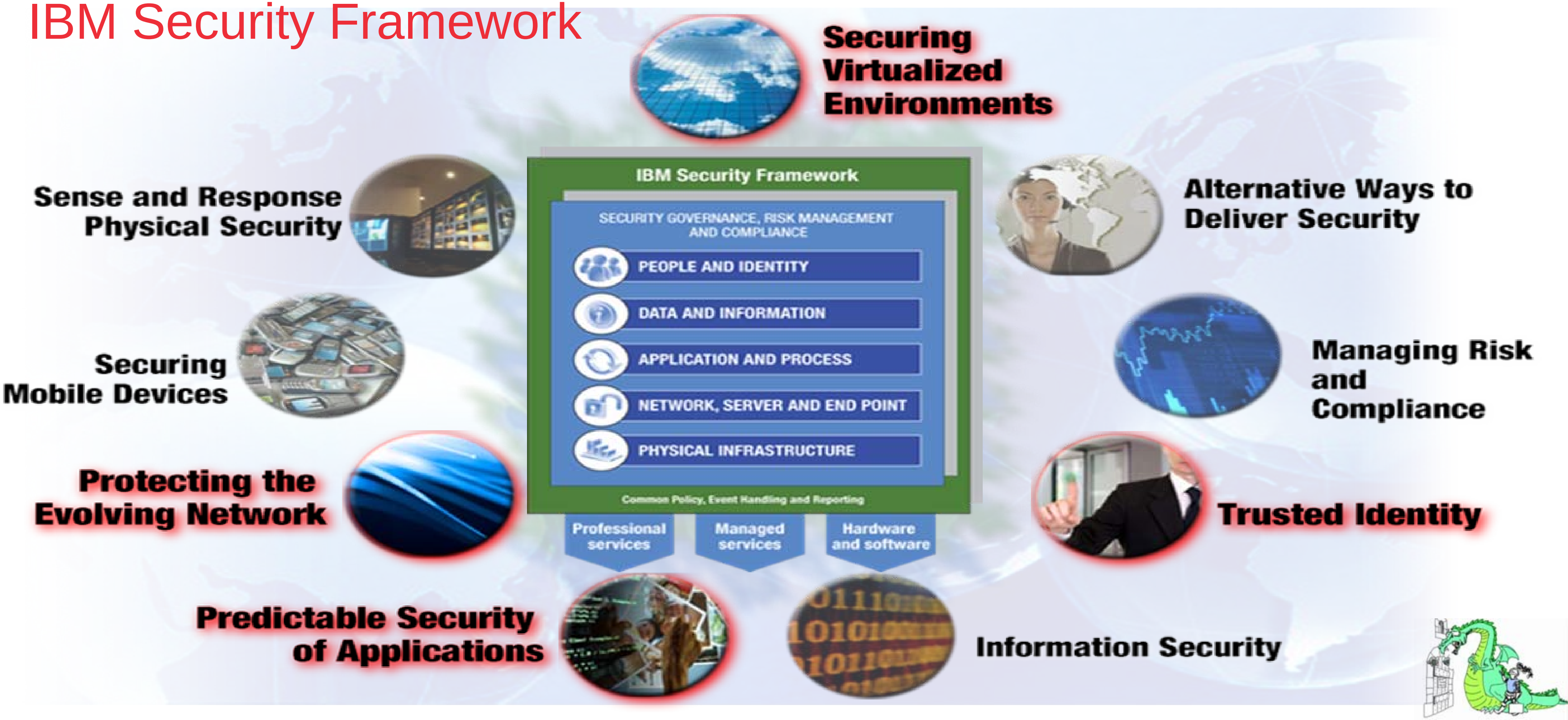
Physical asset management
- Asset management
- Document management

Personnel security

Workforce security
- Awareness training
- Code of conduct

- Employment lifecycle management

IBM Security Framework



Securing Virtualized Environments

Sense and Response Physical Security

Alternative Ways to Deliver Security

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

Common Policy, Event Handling and Reporting

Professional services | Managed services | Hardware and software

Securing Mobile Devices

Managing Risk and Compliance

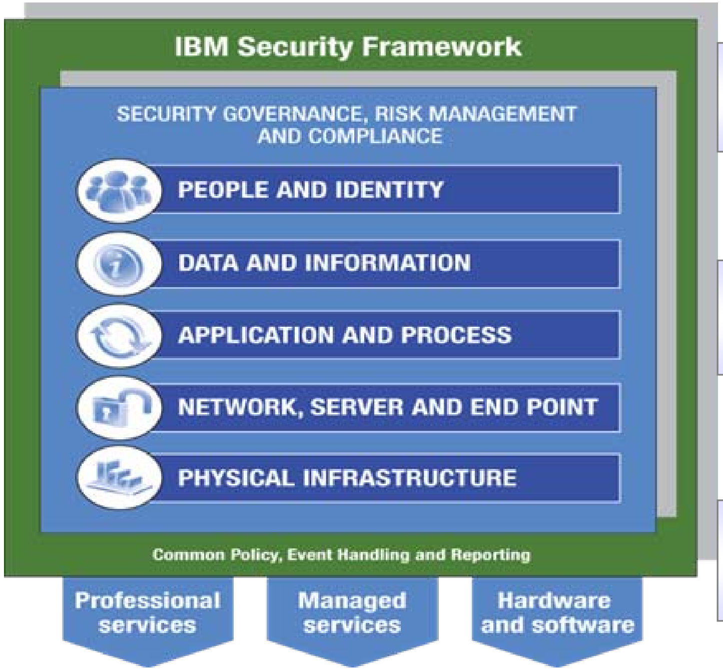
Protecting the Evolving Network

Trusted Identity

Predictable Security of Applications

Information Security

IBM Tivoli Security delivering on the IBM Security Strategy

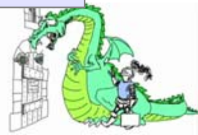


Tivoli Security Strategy and Solutions

Identity, Access & Audit Management → Reduce cost and risk by easing the onboarding and offboarding of users, reporting on user activity

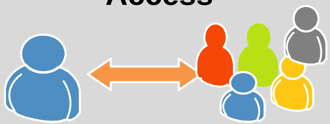
Data & Application Security → Protect business information and reputation by safeguarding data in use or at rest

Enterprise Security Hub → Improve mainframe security administration & enable integrated mainframe & distributed security workloads



PEOPLE AND IDENTITY

Manage Identities and Access



"How can my business benefit from management of digital identity?"

Issues

- Establishing Trusted in Digital Identity
- Cost of administering users and identities in-house
- Privileged user activity unmonitored
- Dormant IDs or shared identities being used to inappropriately access resources
- Role and Entitlements Management

IBM Security Offerings

- ***Identity Lifecycle Management:*** Tivoli Identity and Access Management solutions,
- ***High-Assurance Digital Identities****:* Trusted Identity Initiative
- ***Identity Audit:*** Tivoli Security Compliance Insight Manager, Tivoli zSecure Audit
- Identity & Access Design and Implementation Services
- ISS Managed Identity Services

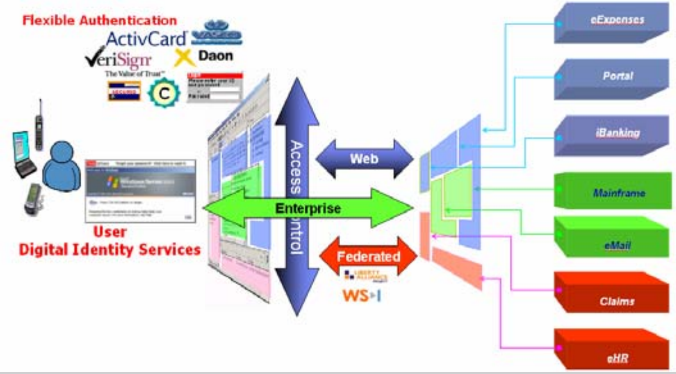
Values

- 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
- Enables shift from traditional brick & mortar sales to delivery of on-line services to customers and partners across the globe
- Single sign-on

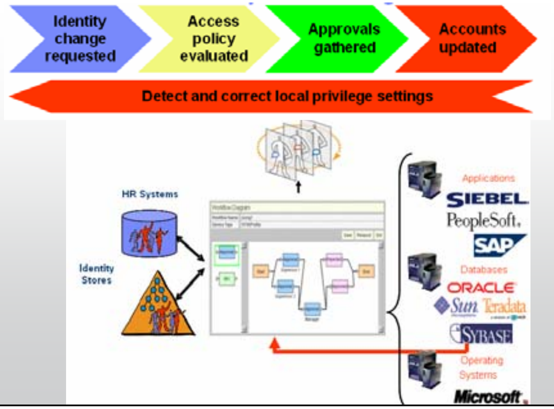
PEOPLE AND IDENTITY

Tivoli Identity and Access assurance

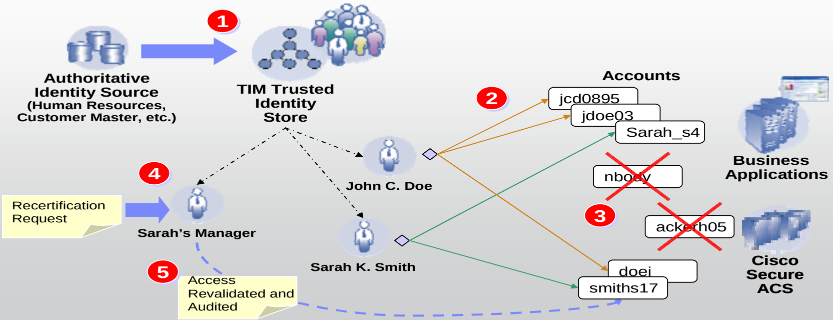
Single Sign On & Password Management



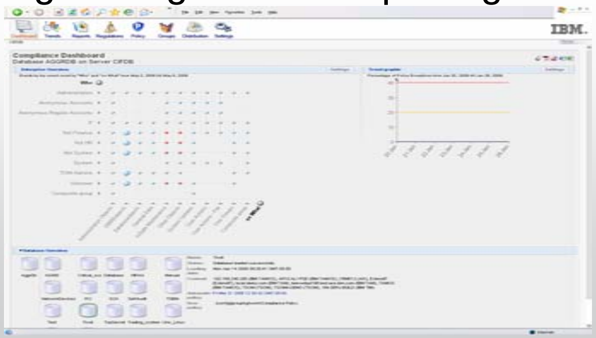
User Provisioning / Role Management



Access Attestation



Security log management & reporting



DATA AND INFORMATION

Protect Data and Information

"How can I reduce the cost and pain associated with tracking and controlling who touched what data when? How do I assure that my data is available to the business, today and tomorrow?"

Issues

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

IBM Security Offerings

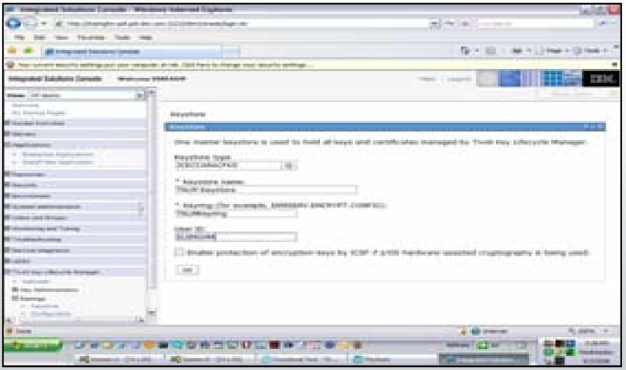
- ISS Data Security and Data Loss Prevention solution
- Tivoli Compliance Insight Manager, ISS SiteProtector, ISS Managed Security Services
- ***Data Encryption****:* Tivoli Key Lifecycle Manager, encrypted tape and disk drives
- ***Data Classification*****:** InfoSphere Information Analyzer, Cognos, FileNet Discovery and Classification
- ***Unstructured Data Security*****:** Tivoli Access Manager
- ***Data Privacy and Masking*****:** Optim Data Privacy Solution
- ISS Professional Security 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
- Data Protection and prevention of Data Loss or Data Leakage
- Decreases number and complexity of controls integrated within the enterprise

Tivoli Data & Application Security Solution

Encrypted Disks & Archive Tapes with Key Management


Integrated Solutions Console - Windows Internet Explorer

Keystore

One master keystore is used to hold all keys and certificates managed by Tivoli Key Lifecycle Manager.

Keystore type:

* Keystore name:
TKLM Keystore

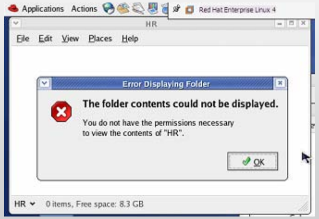
* Keyring (for example, ENNSSERV.ENCRYPT.CONFIG):
TKLMKeyring

User ID:

□ Enable protection of encryption keys by ICSF if z/OS hardware assisted cryptography is being used.

OK

Unstructured Data protection



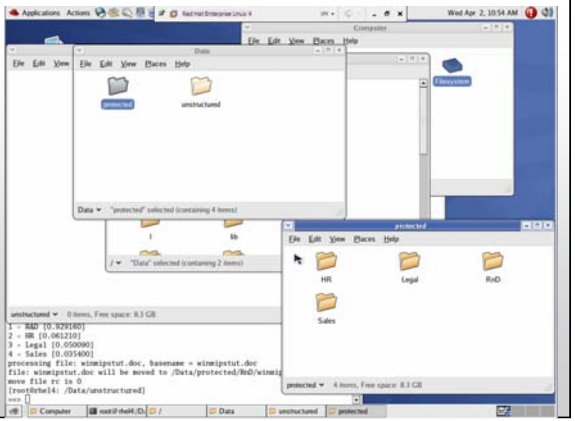
Error Displaying Folder

The folder contents could not be displayed.

You do not have the permissions necessary to view the contents of "HR".

OK

HR ▾ 0 items, Free space: 8.3 GB



Data ▾ "protected" selected (containing 4 items)

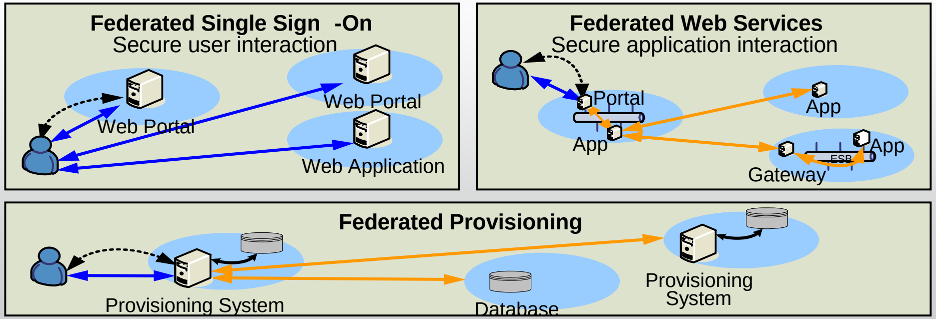
/ ▾ "Data" selected (containing 2 items)

unstructured ▾ 0 items, Free space: 8.3 GB

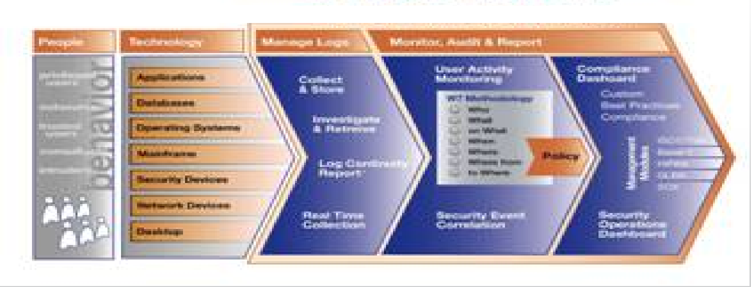
protected ▾ 4 items, Free space: 8.3 GB

```
1 - R&D [0.929160]
2 - HR [0.061210]
3 - Legal [0.050090]
4 - Sales [0.035400]
processing file: winmipstut.doc, basename = winmipstut.doc
file: winmipstut.doc will be moved to /Data/protected/RnD/winmip
move file rc is 0
[root@rhel4: /Data/unstructured]
==> 
```

Portal Security and Federation

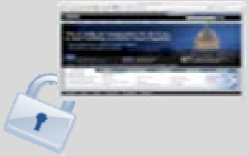


Security log management & reporting



APPLICATION AND PROCESS

Secure Web Applications



"How can my business benefit from management of application security?"

Issues

- Web applications #1 target of hackers
- Applications are deployed with vulnerabilities
- PCI regulatory requirements mandate application security
- Managing fine-grained data entitlements within Apps
- Integrating Distributed and Mainframe security
- Private data exposure in development and test environments

IBM Security Offerings

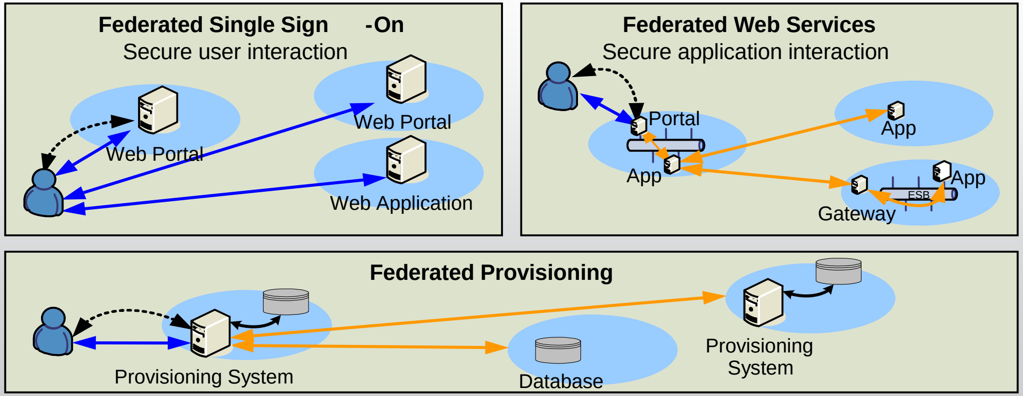
- ***Application Vulnerabilities***: Rational AppScan, ISS Managed Security Services, ISS Application Risk Assessment services
- ***Application Access Controls***: Tivoli Access Manager
- ***Security for SOA***: WebSphere DataPower, Tivoli Security Policy Manager, Tivoli Federated Identity Manager
- ***Messaging Security***: Lotus Domino Messaging, IBM ISS Mail security solutions

Values

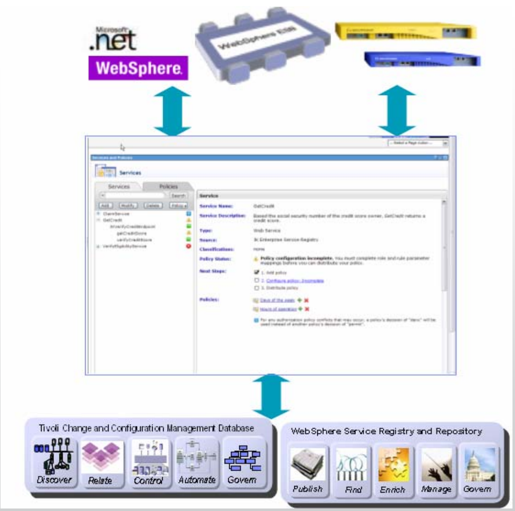
- Reduce risk of outage, defacement or data theft associated with web applications
- Assess and monitor enterprise-wide security policy compliance
- Improve compliance with industry standards and regulatory requirements (e.g., PCI, GLBA, HIPAA, FISMA…)
- Improve ability to integrate business critical applications
- Automated testing and governance throughout the development lifecycle, reducing long-term security costs

APPLICATION AND PROCESS

Portal Security and Federation

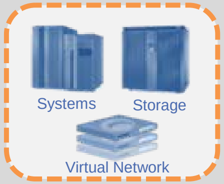


SOA-SharePoint/ DataPower - Policy management



NETWORK, SERVER AND END POINT

Manage Infrastructure Security



“How does my business benefit from infrastructure security protection?”

Issues

- Inability to establish forensic evidence or demonstrate compliance
- Lack of integrated View of Security Information
- Lack of skills to monitor and manage security inputs
- Mass commercialization and automation of threats; Parasitic, stealthier, more damaging attacks
- Poor understanding of risks in new technologies e.g. virtualization and cloud
- Cost managing an ever increasing array of security technologies

IBM Security Offerings

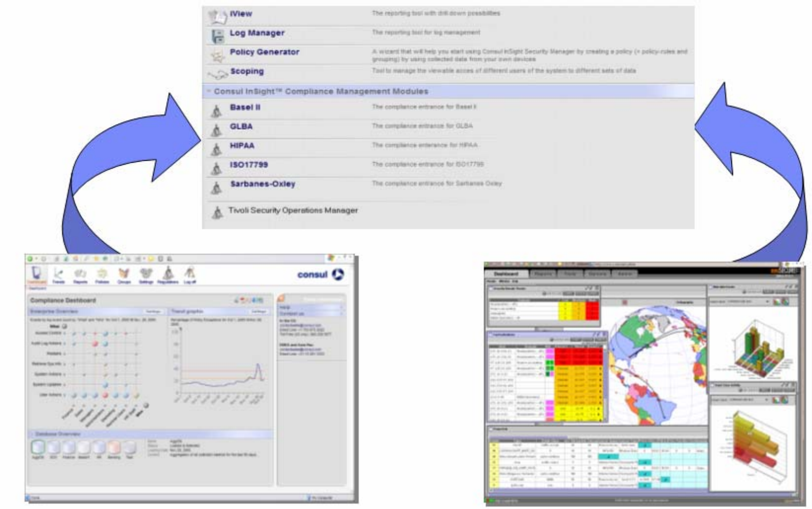
- ***Threat Mitigation***: ISS Network, Server and Endpoint Intrusion Detection and Prevention products powered by X-Force®, Managed Intrusion Prevention and Detection, Network Mail Security, Managed firewall services, Vulnerability Management and Scanning
- ***SIEM***: Tivoli SIEM, Compliance Insight Manager, Security Event and Log Management services
- ***Security Governance***: Regulatory assessments and remediation solutions, Security architecture and policy development
- ***Incident Response***: Incident Management and Emergency Response services
- ***Consulting and Professional Security Services***: Security Intelligence and Advisory Services

Values

- Reduces cost of ongoing management of security operations
- Improves operational availability and assures performance against SLA, backed by industry’s only guaranteed SLA for managed protection services
- Increases productivity by decreasing risk of virus, worm and malcode infestation
- Readily show status against major regulations

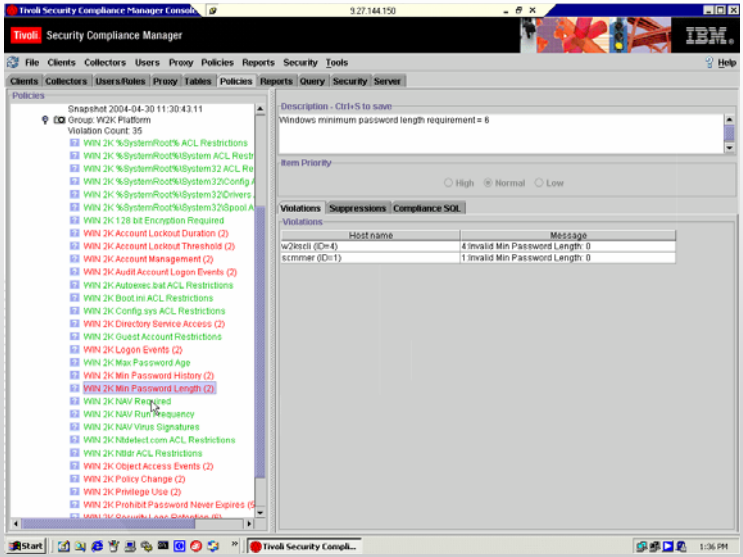
NETWORK, SERVER AND END POINT

Security Information & Event Management



IView	The reporting tool with drill-down possibilities
Log Manager	The reporting tool for log management
Policy Generator	A wizard that will help you start using Consul InSight Security Manager by creating a policy (+ policy-rules and grouping) by using collected data from your own devices
Scoping	Tool to manage the viewable acces of different users of the system to different sets of data
Consul InSight™ Compliance Management Modules	
Basel II	The compliance entrance for Basel II
GLBA	The compliance entrance for GLBA
HIPAA	The compliance enterance for HIPAA
ISO17799	The compliance entrance for ISO17799
Sarbanes-Oxley	The compliance entrance for Sarbanes Oxley
Tivoli Security Operations Manager	

Hardware Security Compliance



Tivoli Security Compliance Manager Console
9.27.144.150
Tivoli Security Compliance Manager
IBM
File Clients Collectors Users Proxy Policies Reports Security Tools Help
Clients Collectors Users/Roles Proxy Tables Policies Reports Query Security Server
Policies
Start
Tivoli Security Compli...
1:36 PM

Snapshot 2004-04-30 11:30:43.11
Group: W2K Platform
Violation Count: 35

- WIN 2K %SystemRoot% ACL Restrictions
- WIN 2K %SystemRoot%\System ACL Restr
- WIN 2K %SystemRoot%\System32 ACL Re
- WIN 2K %SystemRoot%\System32\Config A
- WIN 2K %SystemRoot%\System32\Drivers A
- WIN 2K %SystemRoot%\System32\Spool A
- WIN 2K 128 bit Encryption Required
- WIN 2K Account Lockout Duration (2)
- WIN 2K Account Lockout Threshold (2)
- WIN 2K Account Management (2)
- WIN 2K Audit Account Logon Events (2)
- WIN 2K Autoexec.bat ACL Restrictions
- WIN 2K Boot.ini ACL Restrictions
- WIN 2K Config.sys ACL Restrictions
- WIN 2K Directory Service Access (2)
- WIN 2K Guest Account Restrictions
- WIN 2K Logon Events (2)
- WIN 2K Max Password Age
- WIN 2K Min Password History (2)
- WIN 2K Min Password Length (2)
- WIN 2K NAV Required
- WIN 2K NAV Run Frequency
- WIN 2K NAV Virus Signatures
- WIN 2K Ntdetect.com ACL Restrictions
- WIN 2K Ntldr ACL Restrictions
- WIN 2K Object Access Events (2)
- WIN 2K Policy Change (2)
- WIN 2K Privilege Use (2)
- WIN 2K Prohibit Password Never Expires (5
- WIN 2K Security Logs Retention (6)

Description - Ctrl+S to save

Windows minimum password length requirement = 6

Item Priority

○ High ● Normal ○ Low

Violations | Suppressions | Compliance SQL

Violations

Host name	Message
w2ksdi (ID=4)	4:invalid Min Password Length: 0
scmmer (ID=1)	1:invalid Min Password Length: 0

Gartner's security risks of cloud computing
Privileged User Access
Data Segregation
Data Recovery
Investigative Support
Regulatory Compliance
Data Location
Disaster Recovery

Updates since 2008……….

PEOPLE AND IDENTITY

- New release of Tivoli Access Manager ESSO offers two-factor authentication, Access and Security workflow automation and User Access Tracking & Audit
- Updated Tivoli Compliance Insight Manager offers new compliance modules for FISMA, PCI,ISO 27001
- Increased auditing & compliance capabilities including New RACF classes for installation-defined health checks and WebSphere MQ

DATA AND INFORMATION

- **NEW**: Tivoli Key Lifecycle Manager, simplifies configuration and administration of key generation and management
- ISS Data Security Solutions includes network and endpoint data protection solutions

APPLICATION AND PROCESS

- **NEW**: Tivoli Security Policy Manager, provides unified SOA security policy management & enforcement
- Enable fine-grained authorization and control data entitlements

NETWORK, SERVER AND END POINT

- Tivoli Security Information Event Manager

Business issues

Identity and Access Assurance

- Administers, secures and monitors identities, roles, and entitlements.

Security Management for z/OS

- Simplifies and comprehensively addresses mainframe administration.
- Policy-based user management, security monitoring and compliance reporting on the mainframe.

Data and Application Security

- Provides end-to-end protection of sensitive data, critical applications, and secure storage to address customer’s growing security and compliance challenges.

Solutions

IBM Tivoli Identity and Access Assurance

- Tivoli Identity Manager
- Tivoli Unified Single Sign-On
- Tivoli Access Manager for OS
- Tivoli Compliance Insight Manager

IBM Tivoli Security Management for z/OS

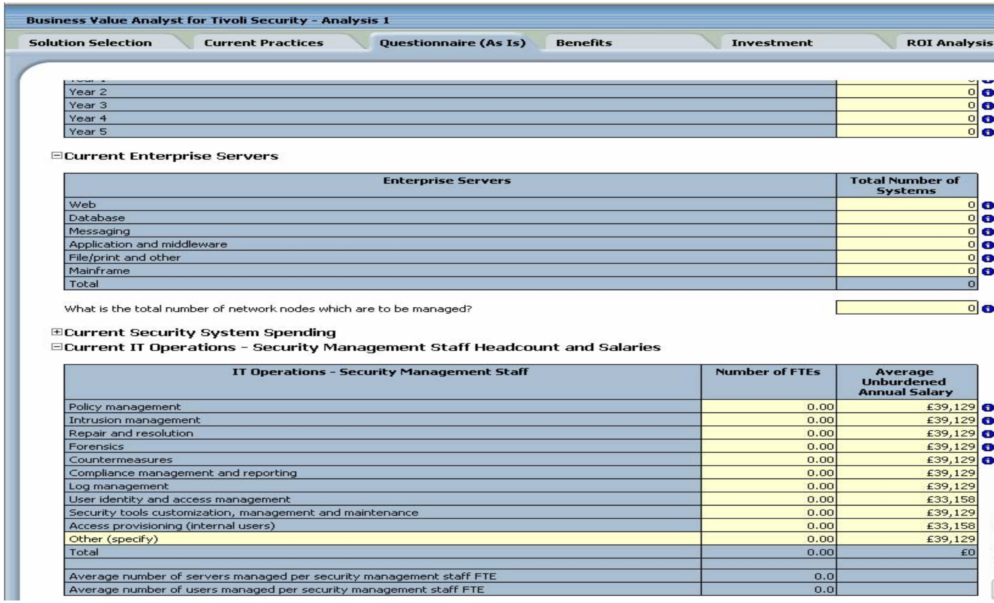
- zSecure Admin
- zSecure Audit for RACF
- zSecure Command Verifier
- Tivoli Compliance Insight Manager

IBM Tivoli Data and Application Security

- Tivoli Security Policy Manager
- Tivoli Key Lifecycle Manager
- Tivoli Compliance Insight Mgr.
- Tivoli Access Manager for OS
- Tivoli Federated Identity Manager

Business Case?

ROI Tool



Business Value Analyst for Tivoli Security - Analysis 1

Year 2	0
Year 3	0
Year 4	0
Year 5	0

⊟Current Enterprise Servers

Enterprise Servers	Total Number of Systems
Web	0
Database	0
Messaging	0
Application and middleware	0
File/print and other	0
Mainframe	0
Total	0

What is the total number of network nodes which are to be managed? 0

⊞Current Security System Spending

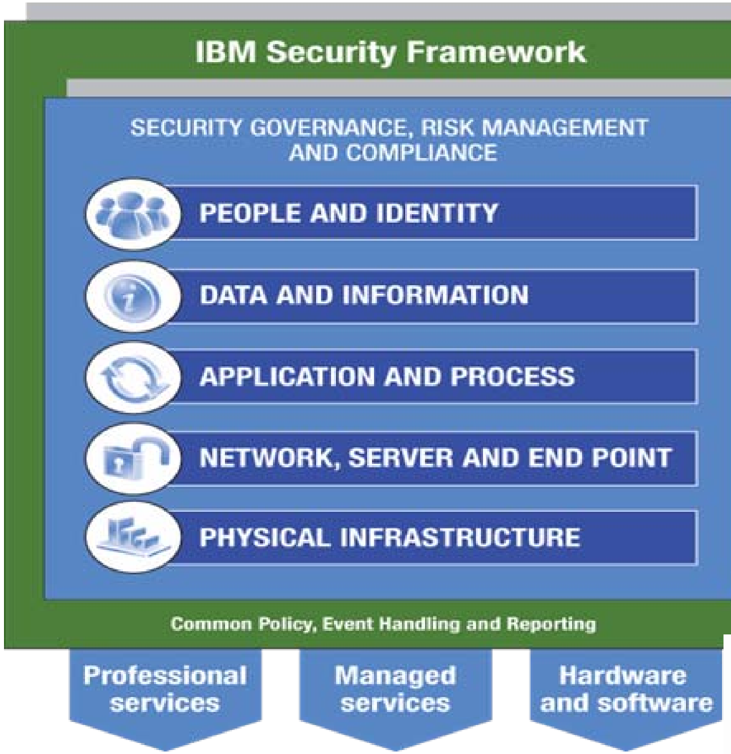
⊟Current IT Operations - Security Management Staff Headcount and Salaries

IT Operations - Security Management Staff	Number of FTEs	Average Unburdened Annual Salary
Policy management	0.00	£39,129
Intrusion management	0.00	£39,129
Repair and resolution	0.00	£39,129
Forensics	0.00	£39,129
Countermeasures	0.00	£39,129
Compliance management and reporting	0.00	£39,129
Log management	0.00	£39,129
User identity and access management	0.00	£33,158
Security tools customization, management and maintenance	0.00	£39,129
Access provisioning (internal users)	0.00	£33,158
Other (specify)	0.00	£39,129
Total	0.00	£0
Average number of servers managed per security management staff FTE	0.0	
Average number of users managed per security management staff FTE	0.0	

IBM Security

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 zSeries environment
- Already managing more than 2.5B security events per day for clients
- **$1.5 Billion** security spend in 2008

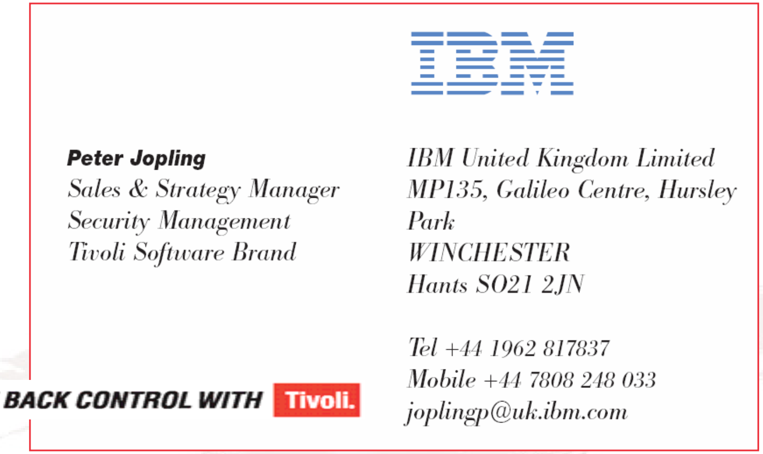


Pulse

Comes to You 2009

ibm.com/software/Tivoli

Managing the World's Infrastructure



IBM

Peter Jopling
Sales & Strategy Manager
Security Management
Tivoli Software Brand

IBM United Kingdom Limited
MP135, Galileo Centre, Hursley Park
WINCHESTER
Hants SO21 2JN

Tel +44 1962 817837
Mobile +44 7808 248 033
joplingp@uk.ibm.com

TAKE BACK CONTROL WITH Tivoli.

The King, the Dragon and the Secure Cloud

http://www.youtube.com/watch?v=jev-YI0MJcw