



IBM Security Forum
Soluções para um ambiente seguro

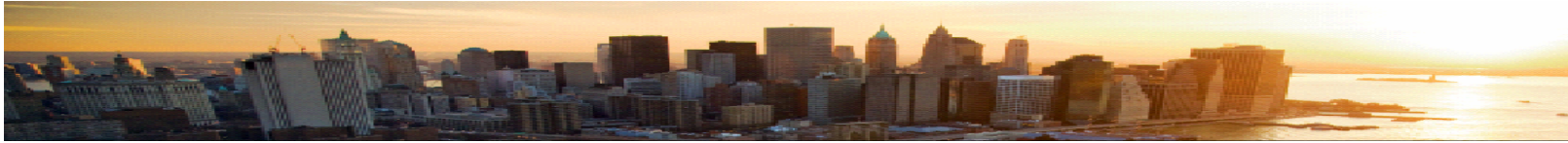




IBM Security Forum
Soluções para um ambiente seguro

Everyday Security:
Simple Solutions to Complex Security Problems

Kristin Lovejoy
Director, Corporate Security Strategy, IBM
klovejoy@us.ibm.com



The world continues to get flatter, smaller and...

...more interconnected through forces such as free trade, the Internet and globalization.

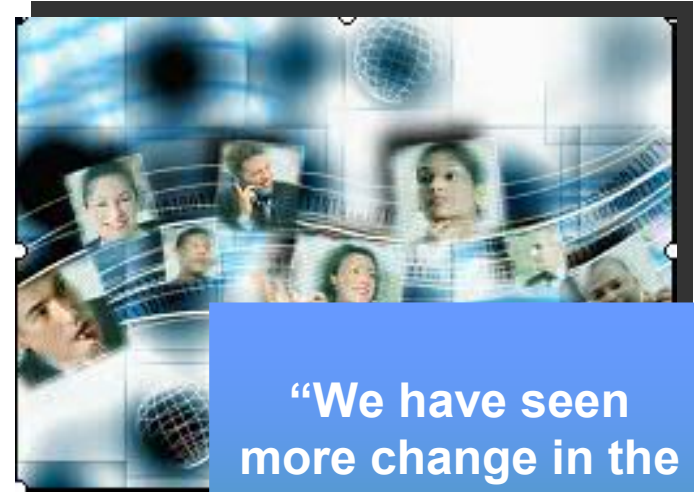
- Review key trends
- Discuss security challenges
- IBM's point of view





Global market forces are impacting us all

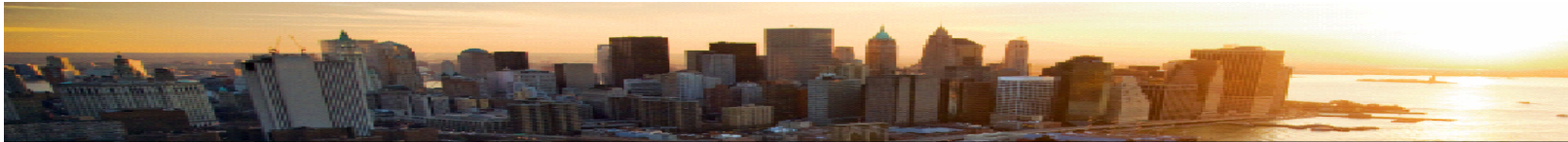
- Reality of living in a globally integrated world
 - Widespread impact of economic downturn and uncertainty
 - Energy shortfalls and erratic commodity prices
 - New customer demands and business models
 - Information explosion and risk/opportunity growth
- Businesses are under increasing pressure to effectively:
 - Manage operational cost and complexity
 - Deliver continuous and high-quality service
 - Address security risks intensified by innovation, emerging technologies, data/information explosion, etc.



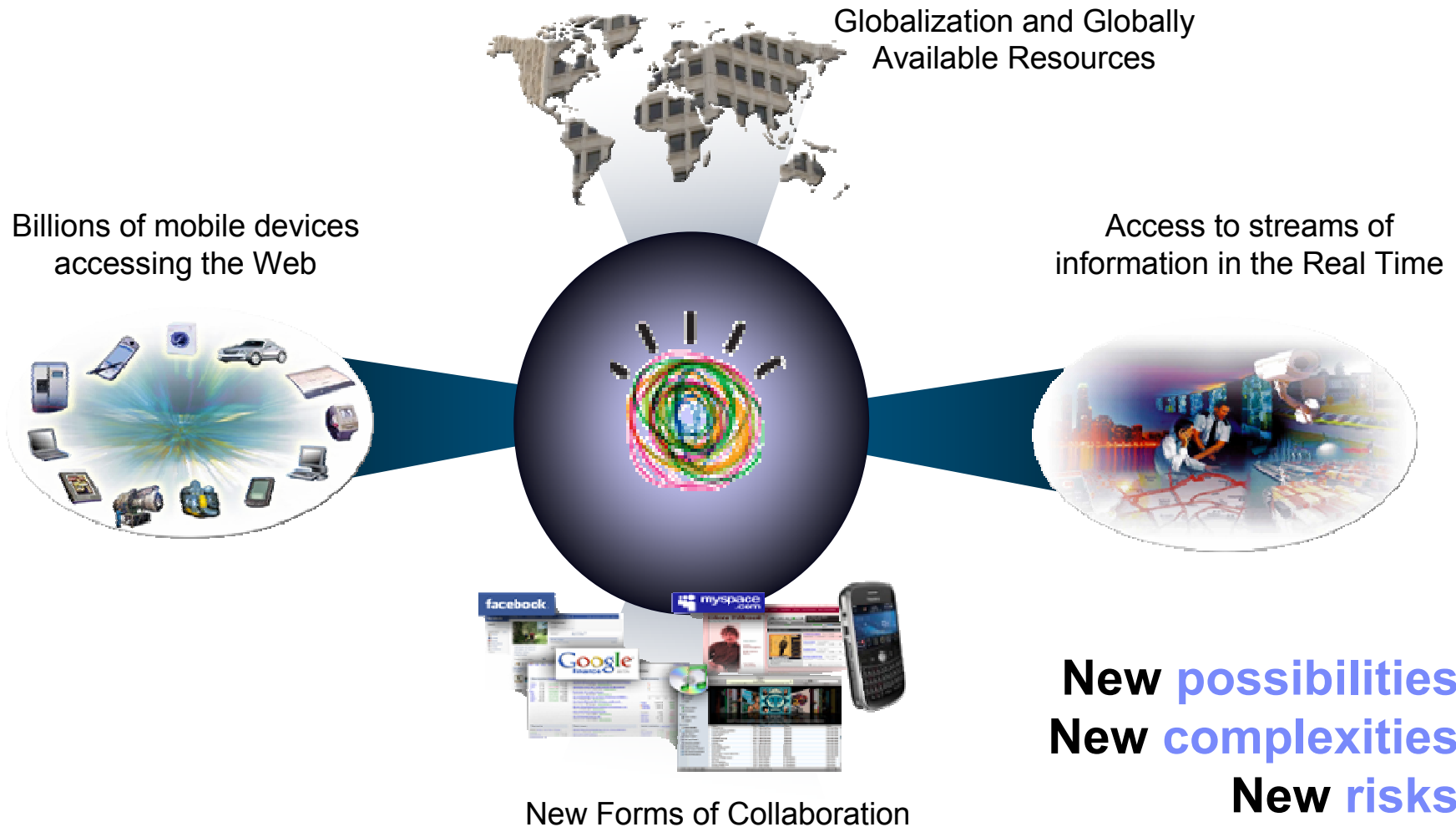
“We have seen more change in the last 10 years than in the previous 90.”

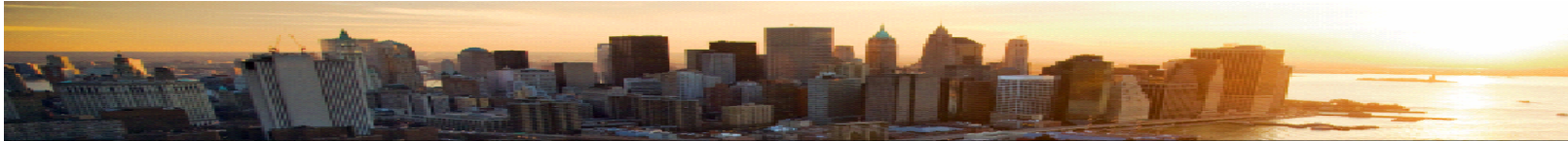
Ad J. Scheepbouwer,
CEO, KPN Telecom

**The planet is getting
instrumented, interconnected and intelligent.**



Welcome to the *smart planet... and a smarter infrastructure*





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



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

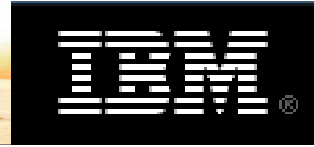
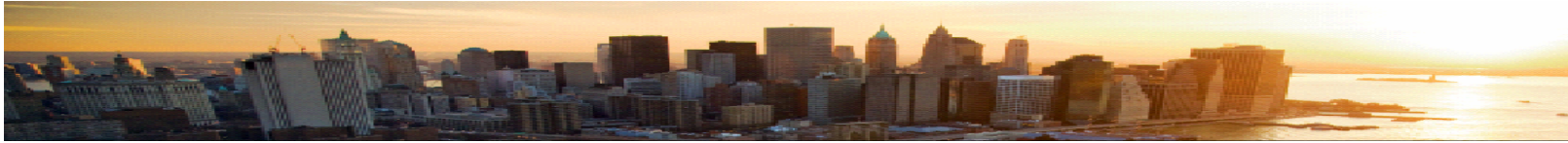
- An assumption or expectation now exists to integrate security into the infrastructure, processes and applications to maintain privacy.



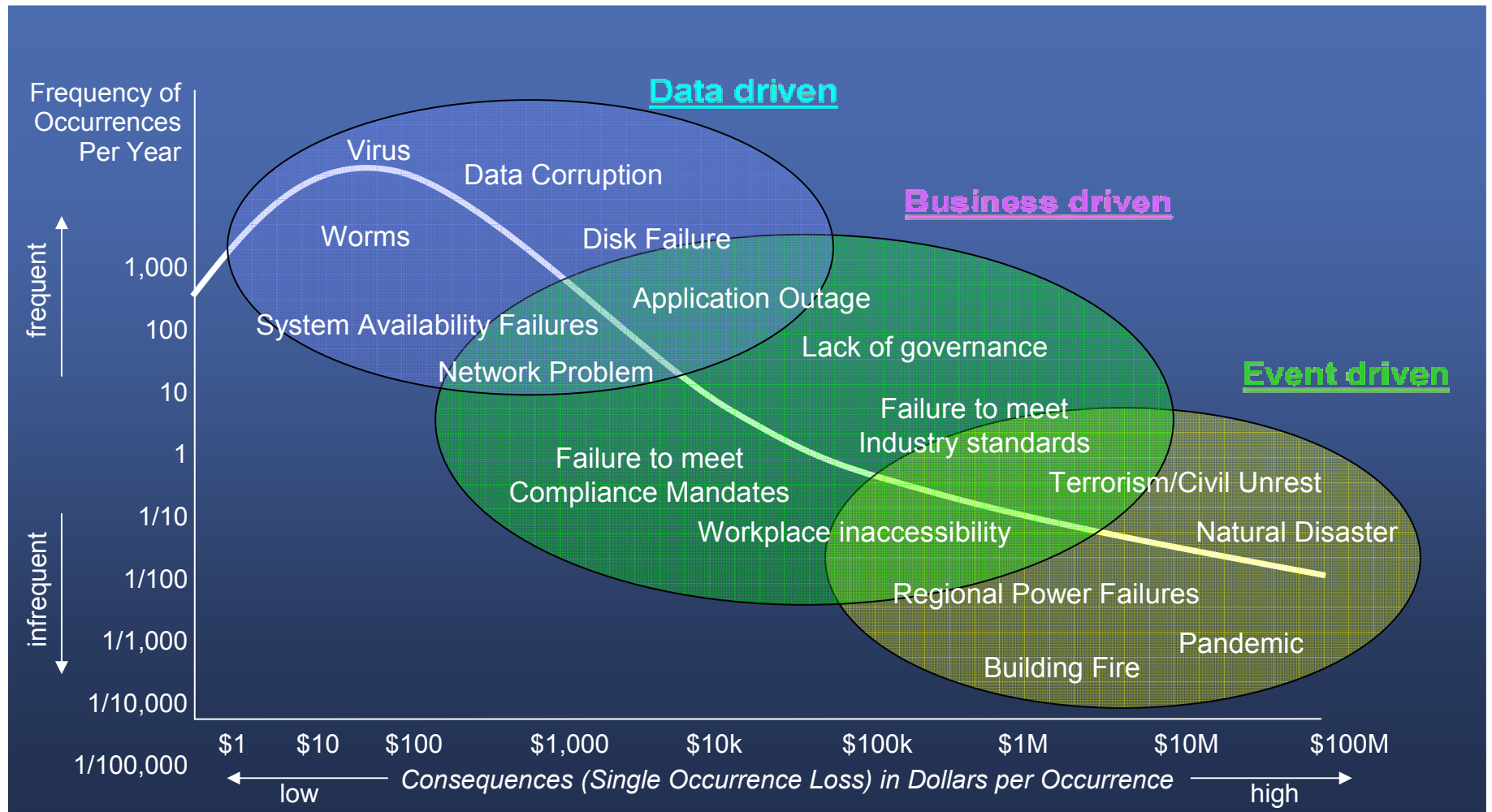
Compliance fatigue

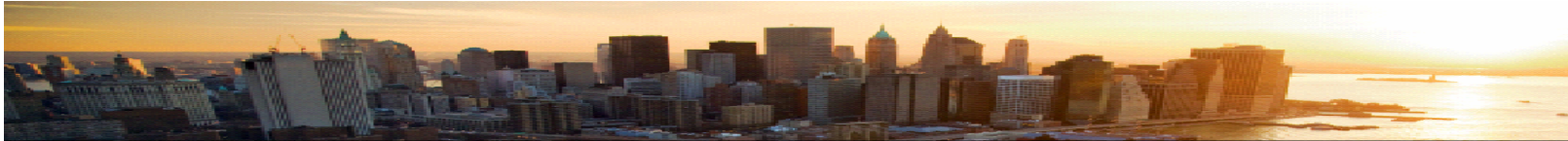
- Organizations are trying to maintain a balance between investing in both the security and compliance postures.

**Source: Pyramid Research, October 2007*



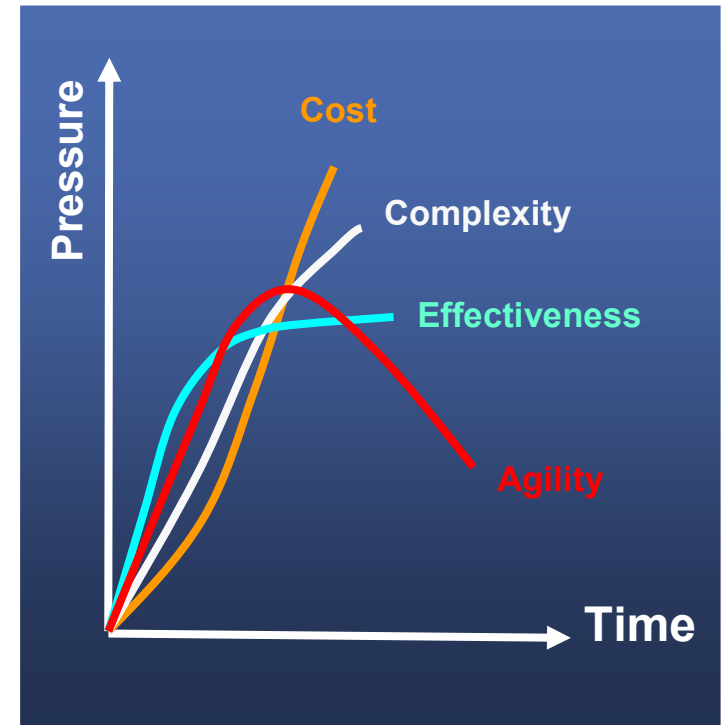
Not all security risks are created equal



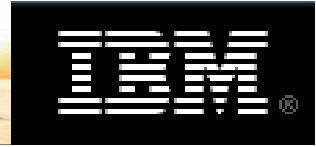


Neither are all security solutions...

- 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*

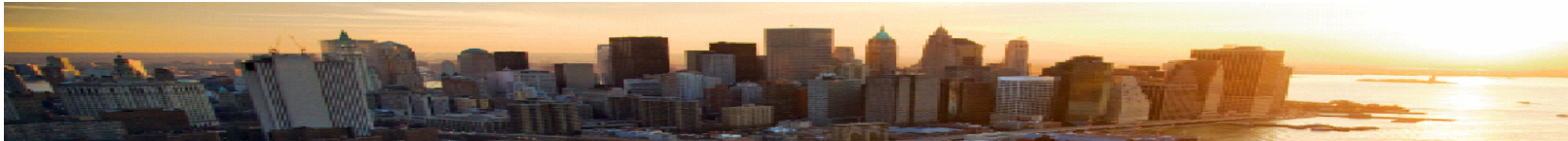


**Sources: W.H. Baker, C.D. Hylender, J.A. Valentine, 2008 Data Breach Investigations Report, Verizon Business, June 2008
ITPI: IT Process Institute, EMA December 2008*



The Solution: *Look at Business as a “System”, and apply security to the logical breakpoints...*



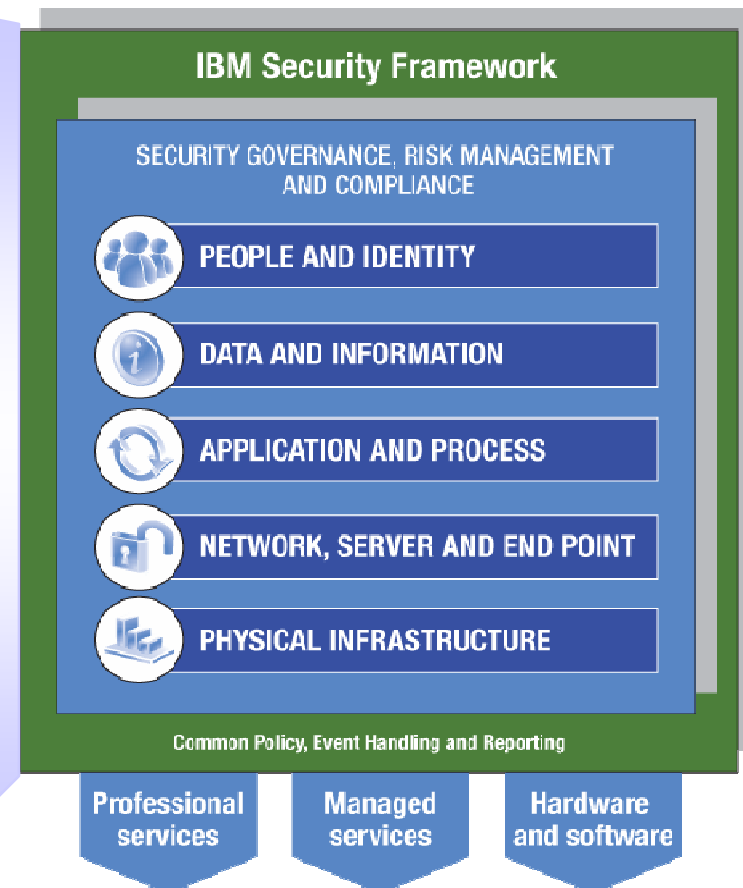


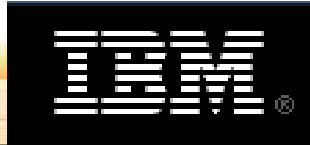
Assure the solidity of your security foundation

Critical Controls

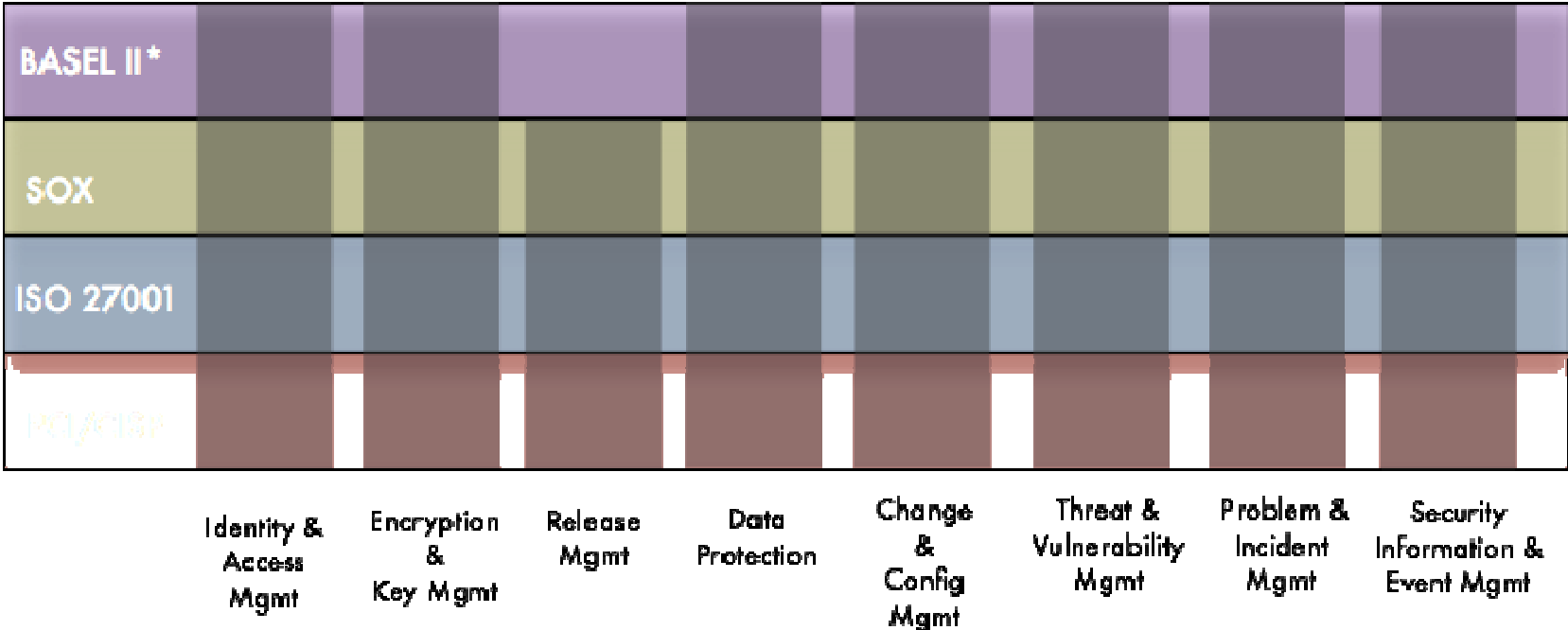
<u>Identity & Access Management</u>	Process for assuring access to enterprise resources has been given to the right people, at the right time
<u>Encryption and Key Management</u>	Capability enabling use of pre-existing investments by providing central management of encryption keys
<u>Database Protection</u>	Capability that allows for granular protection of data in test and production databases
<u>Release Management</u>	Process for assuring efficiency and integrity of the software development lifecycle
<u>Change & Configuration Management</u>	Process for assuring routine, emergency and out-of-band changes are made efficiently, and in such a manner as to prevent operational outages.
<u>Threat & Vulnerability Management</u>	Process and capabilities designed to protect the enterprise infrastructure from new and emerging threats
<u>Problem & Incident Management</u>	Automated workflow and Service Desk designed to assure incidents are escalated and addressed in a timely manner
<u>Security Information & Event Management</u>	Automated log management, monitor and report security and compliance posture

IBM Solutions

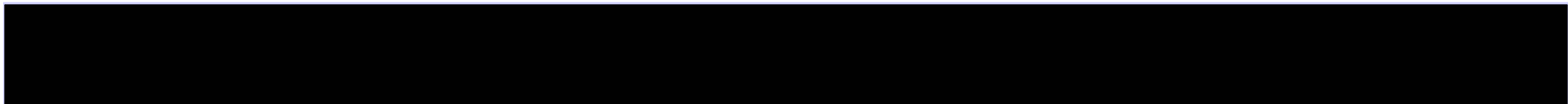


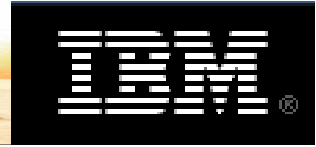
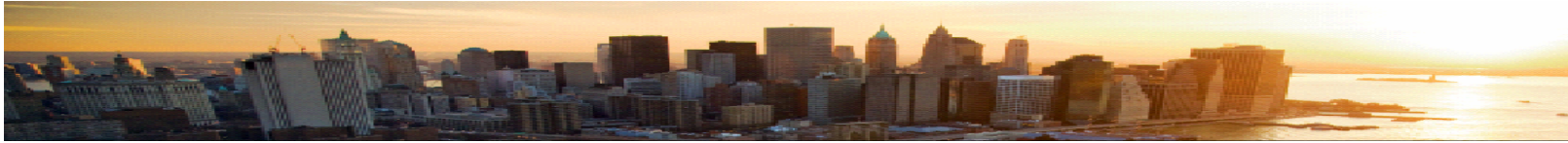


Critical Controls support multiple compliance initiatives



***Basel II is NOT prescriptive, instead it required adoption of an integrated control framework**

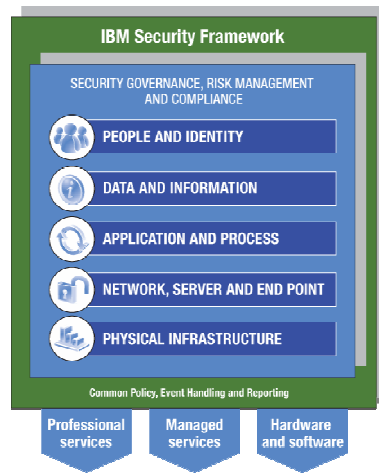




Where do I begin? IBM can help you chart the course...

- Understand your security readiness, using a capability maturity model, across the IT security domains
- Develop a ranked security roadmap to address critical security processes
- Balance your security focus and investment

IBM can help...



Protect sensitive information

1. Assess your organization's security readiness and compliance against industry standards.

2. Identify and prioritize security risks based on business impact and likelihood.

3. Implement security controls to mitigate risks and ensure compliance.

4. Monitor and manage security risks continuously.

5. Report security risks to management and stakeholders.

6. Review and update security controls regularly.

7. Assess your organization's security readiness and compliance against industry standards.

8. Identify and prioritize security risks based on business impact and likelihood.

9. Implement security controls to mitigate risks and ensure compliance.

10. Monitor and manage security risks continuously.

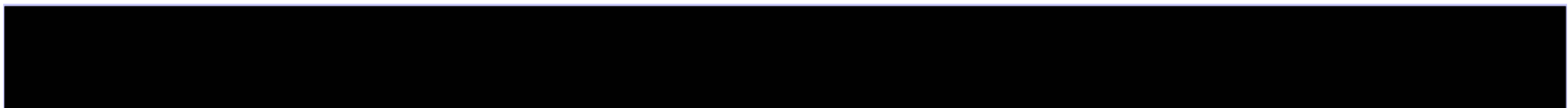
11. Report security risks to management and stakeholders.

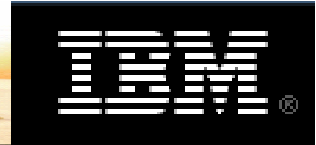
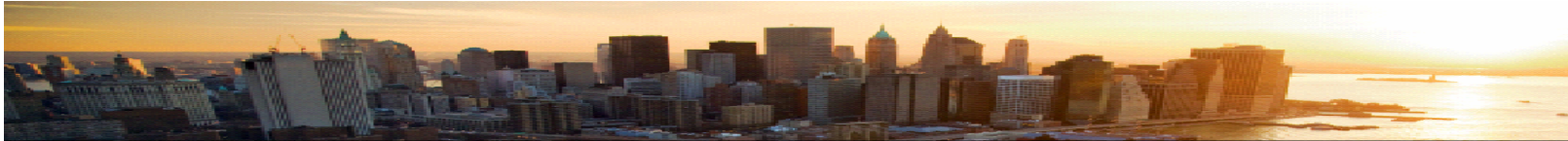
12. Review and update security controls regularly.

Security Report Card

Assessment: This report card provides a snapshot of your organization's security readiness. It highlights areas for improvement and provides a ranked list of security risks. The report card is based on the results of the security assessment and is updated regularly.

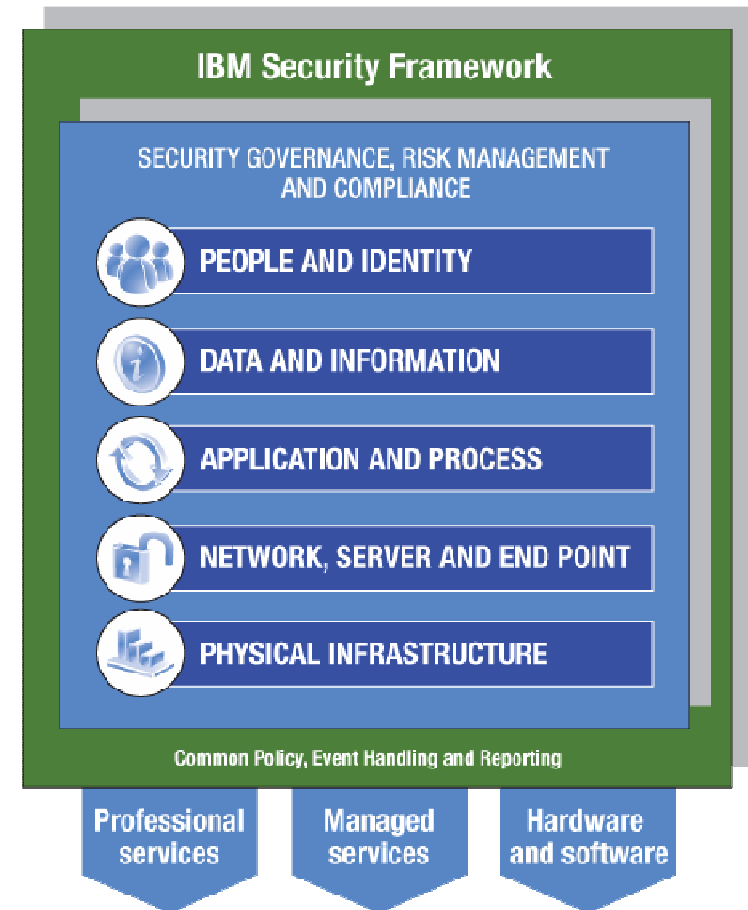
My Security

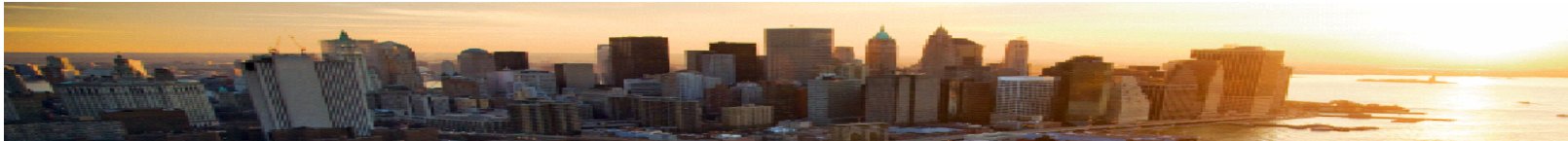




IBM: Comprehensive Security Risk & Compliance Management

- The *only security vendor* in the market with *complete coverage of the security foundation*
- 15,000 researchers, developers and SMEs on security initiatives, including the world-renowned *ISS x-Force*
- 3,000+ security & risk management patents
- Hundreds of security customer references
- 40+ years of proven success securing the zSeries environment
- \$1.5 Billion security spend in 2008

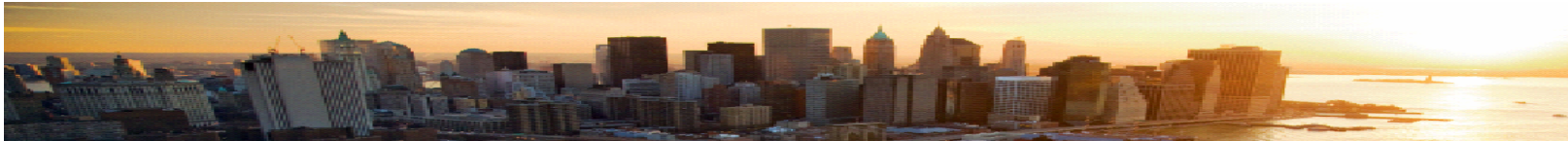




IBM Global Security Reach



IBM has the unmatched global and local expertise to deliver complete solutions – and manage the cost and complexity of security



Customer success stories

A collage of logos for various IBM customers, arranged around a central graphic of the IBM Security Framework. The logos include:

- enresa (Empresa Nacional de Residuos Radiactivos, S. A.)
- Borregaard
- NAYANA COMMUNICATION
- Washington Trust Bank
- Australian Open
- cmc (community medical care)
- DukeMedicine
- GODIVA Chocolatier
- CONVERGENCE CT
- GLOBAL DATA VAULTING
- arek
- HUGHES
- Mercantil
- IBM
- AGENTRICS
- Mⁿ Services
- bp
- POLICE DEPARTMENT WEST HAVEN CONNECTICUT
- BAYLOR UNIVERSITY
- STADTWERKE ILMENAU GMBH (STROM • ERGAS)
- MIYA Clinical Research and Development
- DTCC
- Trillium HEALTH CENTRE
- THE INTERNATIONAL BANK OF MIAMI, N.A.
- P&G
- NORTHWEST HOSPITAL & MEDICAL CENTER
- ZOO ATLANTA
- WestLB
- Hbc

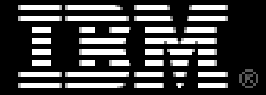
IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

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

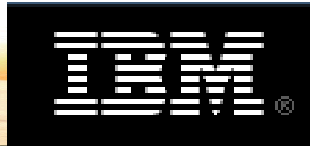
Common Policy, Event Handling and Reporting

- Professional services
- Managed services
- Hardware and software

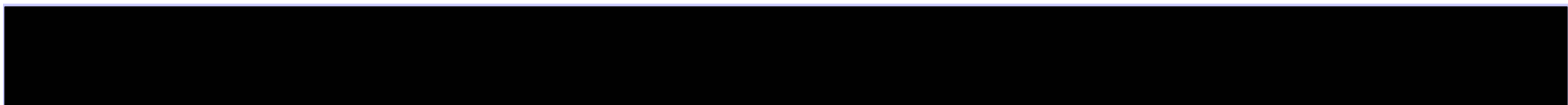


Disclaimer

- The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



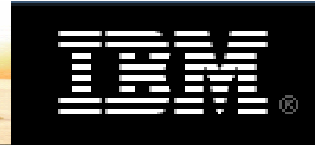
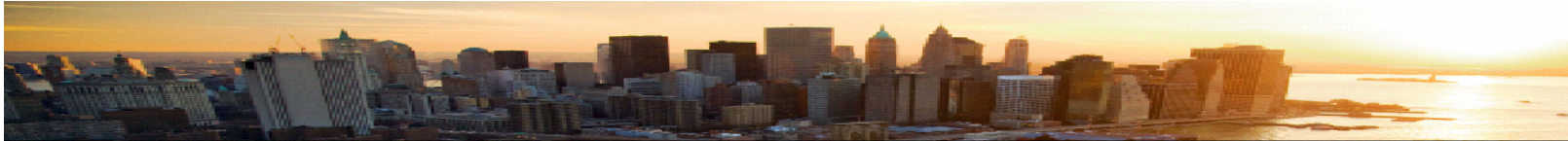
Thank
You





Risks Details

Silde 5 includes links to the slides in this section)



Client results

Hudson's Bay Company

- Anticipates, tracks and mitigates security threats before they cause harm to data or the IT infrastructure.
- Provides professional management of network devices.

✓ *"IBM provided us with more than just compliance. Sensitive data is secure, systems are monitored closely for performance issues, and our IT staff can focus more mission-critical activities."*

DTCC

- Security features are designed and built into more than 225 new applications per year.
- Help improved developer productivity.
- Reduced time to market for each new service.

✓ *"The real key is that we have the education in place and now implement security early in the application development lifecycle, so we have less overall vulnerabilities to manage."*

Community Medical Centers

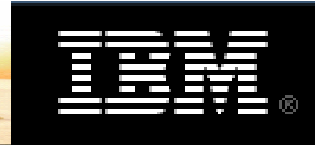
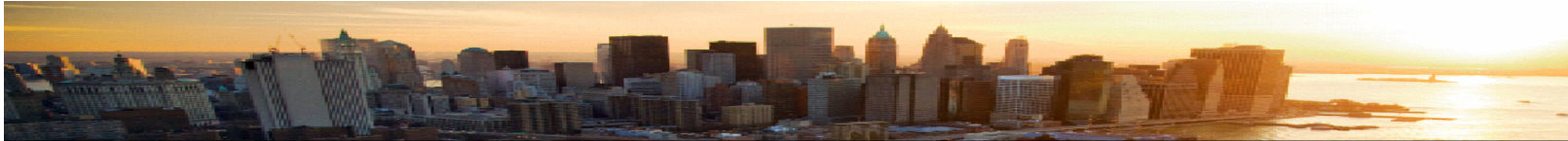
- Reduced costs with fewer password resets and simplified administration.
- Enhanced security through HIPAA support.
- Improved staff productivity with single sign-on support.

✓ *"Tivoli Access Manager for Enterprise Single Sign-On provides our users with one secure password to our applications and flexibility to manage how users access applications, something other vendors have not easily been able to provide."*

Allianz Seguros

- Applied proven data masking techniques to protect privacy and support compliance with country regulations.

✓ *"After attending a demonstration, the members of our evaluation team agreed that Optim provided the capabilities we needed to improve application development and testing processes and protect privacy,"*



Risk: New technology introduces new security challenges



- Technology innovations, like **virtualization & cloud computing models**, used to enable the globally integrated enterprise increase infrastructure complexity
 - Lack of skills, best practices, industry expertise compounds the security challenge
- **Web 2.0 and SOA** style composite applications introduce a new level of complexity
 - 54% of all vulnerabilities disclosed in 2008 were web-based¹
 - 80% of development costs are spent identifying and correcting defects, costing \$25 during coding phase vs. \$16,000 in post-production²
 - View into application and information level entitlements is needed for regulatory compliance

Web Application Vulnerabilities

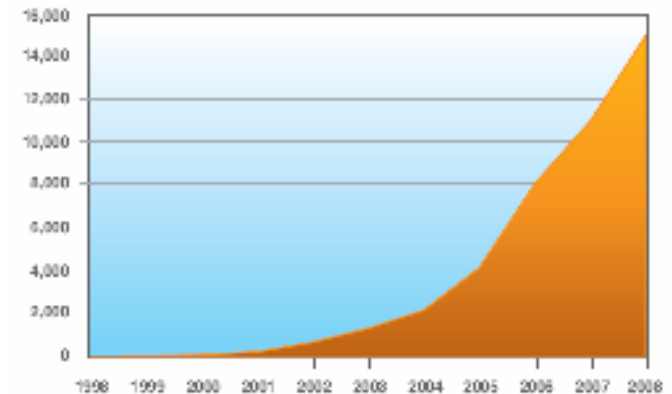


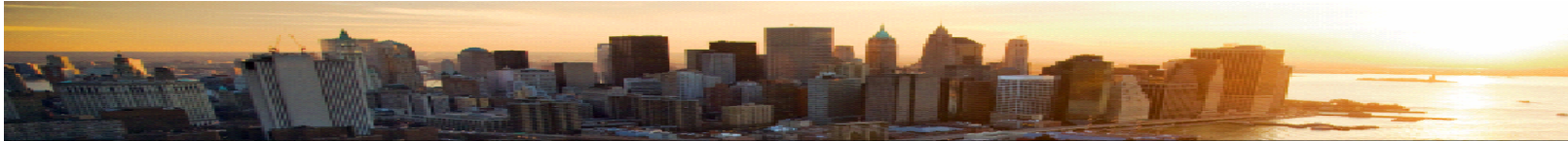
Figure 10: Cumulative Count of Web Application Vulnerabilities, 1998-2008

¹IBM Internet Security Systems: X-Force®
2008 Trend & Risk Report, Jan 2009

²Applied Software Measurement, Caper Jones, 1996

Discussion Question:

- To what extent has introduction of new technologies, like virtualization, changed your approach to security and compliance management?




Risk: Volume of data is exploding

What's driving this tremendous growth?

- Records retention for regulatory and industry compliance
- Data Backup and a Disaster Recovery environment that mirror production data for business resiliency
- Development and test requirements
- Mergers and acquisitions that lead to redundant systems, data centers, applications, etc.



- Technology innovation that makes it possible to access more data, more quickly than ever before

- 
- 🕒 Data volumes double every 18 months¹
 - 🕒 37% of data is expired or inactive²
 - 🕒 Information created, captured, or replicated exceeded available storage for the 1st time in 2007³
 - 🕒 70% of the digital universe is created by individuals³...
 - 🕒 Enterprises are responsible for the security, privacy, reliability & compliance of 85%³
 - 🕒 Data breach costs \$6.6 million on average and more than \$200 per compromised record⁴
 - 🕒 Average US legal discovery request can cost organizations from \$150K to \$250K⁵

¹ "Changing Enterprise Data Profile", IDC, December 2007

² "The Costs of Enterprise Downtime: NA Vertical Markets 2005" International Research; IBM Market Intelligence

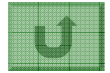
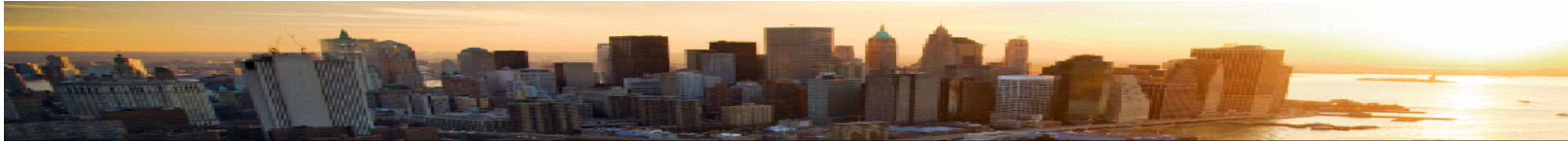
³ "The Diverse and Exploding Digital Universe, IDC, March 2008

⁴ Ponemon Institute, February 2009

⁵ CIO Magazine, Survey 2007

Discussion Question:

- How have you addressed the information explosion?



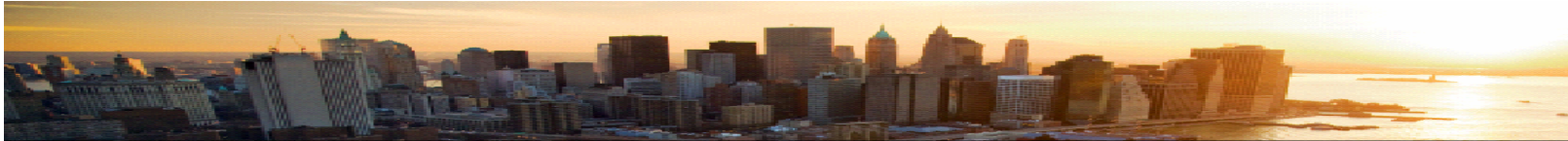
Risk: Barbarians are everywhere

- Wireless devices empower individuals to more effectively participate in the global economy
 - Able to send and receive information (audio and video)
 - Authentication tool for secure transactions
 - Security technology is many years behind the security used to protect PCs
- Green initiatives lead to increased adoption of telecommuting strategies
 - New breed of security threat: Those that know no geographical boundaries
- Persistent security threat
 - Privileged users with limited skills, following manual process definition, with high levels of physical and logical access

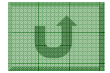


Discussion Question:

- Have you considered how security can enable a 'teleworking' strategy?



Risk: The supply chain is only as strong as the weakest link

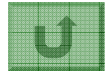
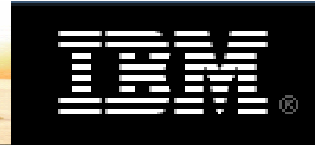


- In an increasingly networked world, enterprises must shore-up their weakest supply chain partners
- Need to collaborate in monitoring end-to-end security and respond to threats in real time
 - More evenly distributed security responsibilities
 - Increased transparency from start to finish
 - Eased burden of customer-facing unit
- Growing number of compliance requirements and industry standards, like the Payment Card Industries Data Security Standard (PCI-DSS), require partners to meet certain minimum requirements



Discussion Question:

- How does your organization ensure each link in the supply chain shoulders their fair share of the load for compliance and the responsibility for failure?



Risk: Expectation of privacy

- Consumer expectation is that security should be built in to services themselves
 - 50% of consumers still avoid online purchases due to fear of financial information being stolen¹
- Expectation drives regulation
- Vendors, like automakers, are expected to take a greater share of responsibility

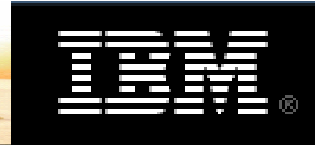
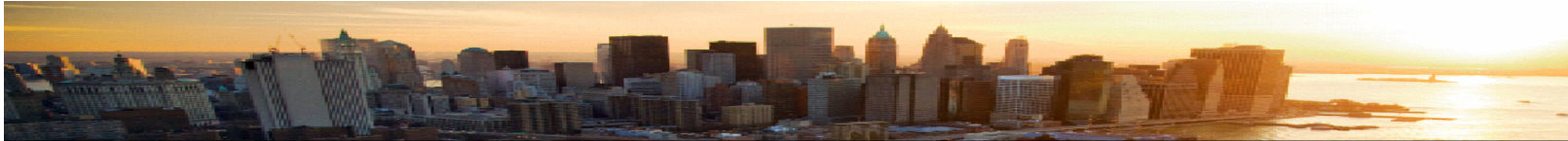


- Critical to assess trade-offs consumers are willing to make against convenience or cost
- Risk of so much security that functionality is lost:
careful not to destroy that which you are trying to protect!

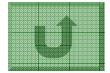
¹Cyber Security Industry Alliance (CSIA) survey, May 2005

Discussion Question:

- To what extent is privacy driving security spend?



Risk: Compliance fatigue

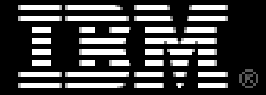


- Complexity and confusion keep customers from acting strategically
 - Extended relationships create a tangle of potential legal liability
 - Compliance requirements are inconsistent within and across geographies
 - Confusion as to where to start
- Pressure to simply “check the box” has resulted in creation of silos
 - Silos lead to duplicative efforts and redundant spending as well as reduced visibility
- The CSO struggles to become a consultant to the business
 - Nearly impossible without a central, risk based view



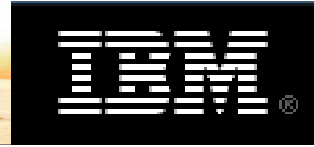
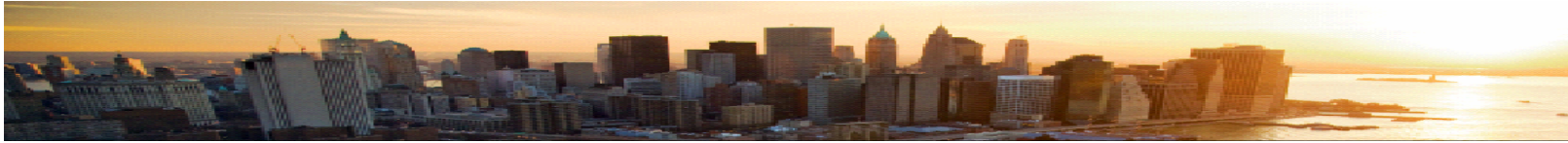
Discussion Question:

- How much security and compliance control is good enough?



Product Back-up slides

Cross-brand solutions highlighted using the
IBM Security Framework as the organizing
principle



PEOPLE AND IDENTITY

Manage Identities and Access



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

Issues

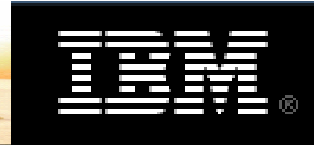
- Understanding the identity risk gap
- Cost of administering users and identities in-house
- Privileged user activity unmonitored
- Dormant IDs or shared identities being used to inappropriately access resources
- Failing an audit

IBM Security Offerings

- **Identity Lifecycle Management:** Tivoli Identity and Access Management solutions,
- **High-Assurance Digital Identities:** Trusted Identity Initiative
- **Identity Audit:** Tivoli 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
- 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



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

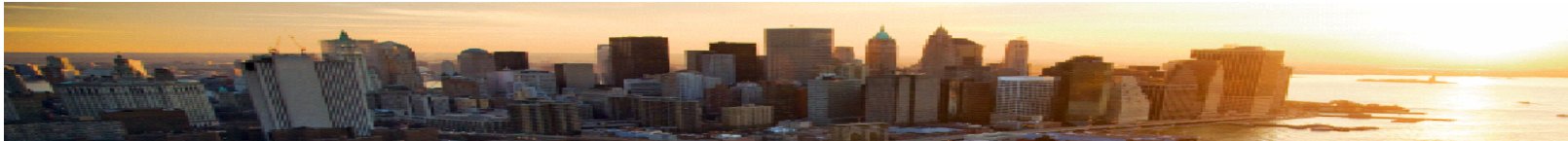
- Data stored on removable media that can be lost/stolen
- Data stored in the clear is easily accessible
- Inconsistent data policies
- Unstructured and/or unencrypted data
- Legal, regulatory and ethical exposure for the organization
- Costs of data breaches, notification, brand value
- Failing an audit

IBM Security Offerings

- ISS Data Security and Data Loss Prevention solution
- **SIEM:** Tivoli Compliance Insight Manager, ISS SiteProtector, ISS Managed Security Services
- **Data Encryption:** Tivoli Key Lifecycle Manager, encrypted tape and disk drives
- **Protecting Data In Motion:** WebSphere MQ Extended Security Edition, WebSphere DataPower SOA Appliances
- **Data Classification:** InfoSphere Information Analyzer, Cognos, Enterprise Content Management, 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
- Assures data is not deliberately or inadvertently taken, leaked, or damaged
- Decreases number and complexity of controls integrated within the enterprise



APPLICATION AND PROCESS

Secure Web Applications



“How can my business benefit from management of application security?”

Issues

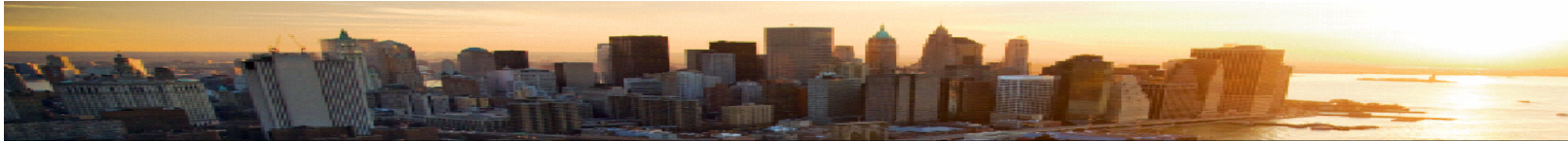
- Web applications #1 target of hackers seeking to exploit vulnerabilities
- Increasing number of attacks via XML scripting and virus insertion
- Applications are deployed with vulnerabilities
- Poor security configs expose clients to business loss
- PCI regulatory requirements mandate application security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

IBM Security Offerings

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

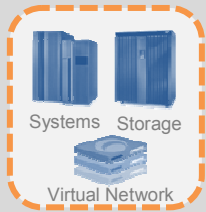
Values

- 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 securely
- Automated testing and governance throughout the development lifecycle, reducing long-term security costs



NETWORK, SERVER AND END POINT

Manage Infrastructure Security



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

Issues

- Mass commercialization and automation of threats
- Parasitic, stealthier, more damaging attacks
- Poor understanding of risks in new technologies and applications, including virtualization and cloud
- Weak application controls
- Lack of skills to monitor and manage security inputs
- Compounding cost of managing an ever increasing array of security technologies
- Undetected breaches due to privilege access misuse and downtime from incidents
- Inability to establish forensic evidence or demonstrate compliance

IBM Security Offerings

- **Threat Mitigation:** ISS Network, WebSphere DataPower SOA Appliances, 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 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 malware infestation
- Decreases volume of incoming spam
- Drill down on specific violations to quickly address resolution
- Readily show status against major regulations