Smarter systems for a Smarter Planet.

The IBM Smarter Government Briefing Series

Briefing 4:

Data Management - Security & Privacy

Enhancing the security and privacy of your sensitive information

Data Protection and Compliance

Mark Johnston – Security Solution Architect

16/10/2011

Introduction

- Mark Johnston is a Security Solution Architect and part of IBM's Worldwide Security Tiger Team within IBM Software Group.

- Mark has been implementing IT Systems for the past 11 years. Since 2005, Mark has consulted with various Australian federal and state government departments and agencies, helping them to build Identity and Access Solutions for their business.

- Recently spent last 2 years in Brisbane working on QLD Government IAM programs of work as part of, IBM Security and Privacy Practice, Global Business Services.

Email : markjohnston@au1.ibm.com
Twitter: markjohnston_au
LinkedIn: http://www.linkedin.com/in/markjohnstonau

Agenda

Learn how IBM security solutions enable organisations to take a holistic approach to protecting information:

- The current threat landscape
- Understanding where sensitive data exists
- Safeguarding sensitive data
- Protecting both production and non-production environments
- Securing and continuously monitoring access to data
- Understand threats and vulnerability awareness using IBM X-Force
- Cover some case studies of IBM clients protecting data

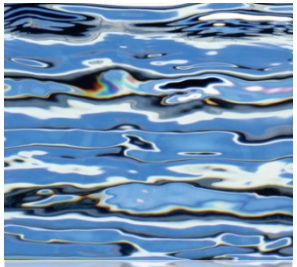
The planet is becoming more instrumented, interconnected, and intelligent creating new Cyber Security challenges

Smart Supply Chains

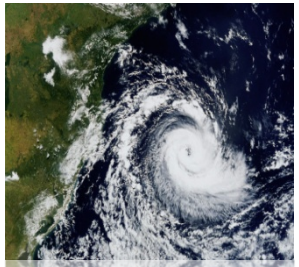
Smart Countries

Smart Retail

Smart Water Management



Smart Weather



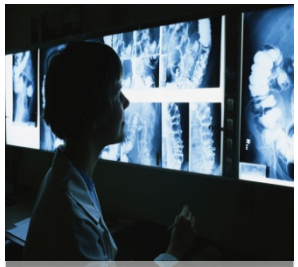
Smart Energy Grids

INSTRUMENTED **INTERCONNECTED** **INTELLIGENT**

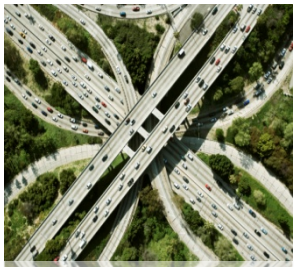
Smart Oil Field Technologies

Smart Regions

Smart Healthcare

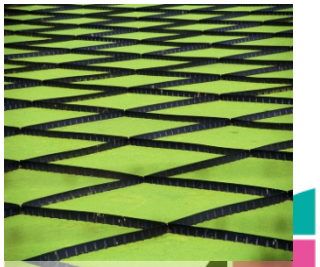


Smart Traffic Systems



Smart Cities

Smart Food Systems



The planet is becoming more instrumented, interconnected, and intelligent creating new Cyber Security challenges

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 was estimated to be **$29.8 billion** in 2010

Ensuring Compliance

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

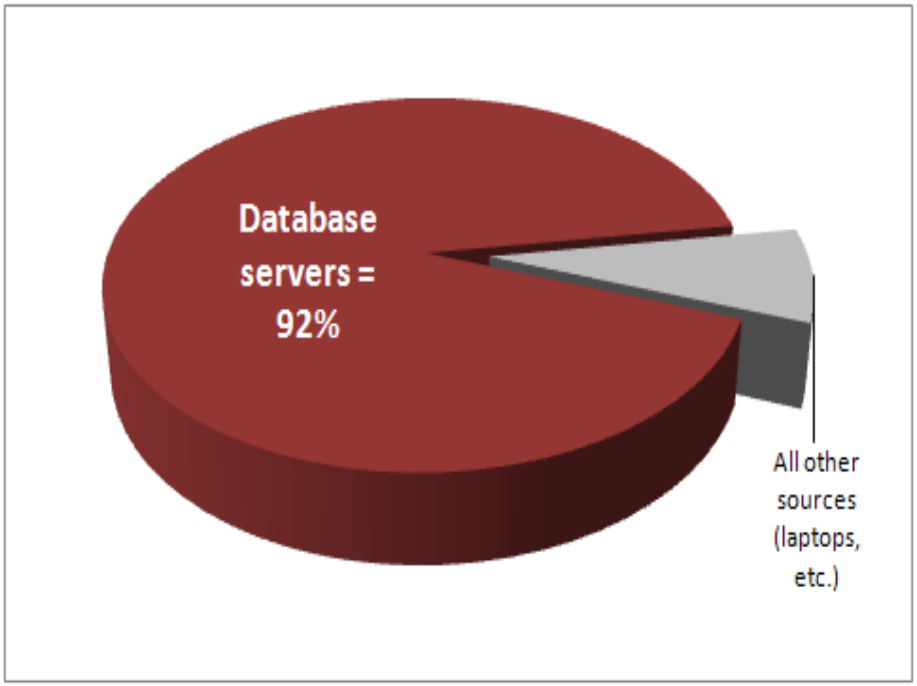
Source **http://searchcompliance.techtarget.com/news/article/0,289142,sid195_gci1375707,00.html**

What's the word here locally, from a public opinion

http://www.zdnet.com.au/wa-govt-slammed-for-sloppy-cybersecurity-339316824.htm?ocid=nl_SEC_16062011_fea_1

Database Servers Are The Primary Source of Breached Data

Source of Breached Records



2010 Data Breach Report from Verizon Business RISK Team

http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf

… up from 75% in 2009 Report

SQL injection played a role in **79% of records compromised** during 2009 breaches

"Although much angst and security funding is given to …. **mobile devices and end-user systems,** these assets **are simply not a major point of compromise."**

Security challenge - Cost, Complexity and Compliance

Emerging technology

Data and information explosion

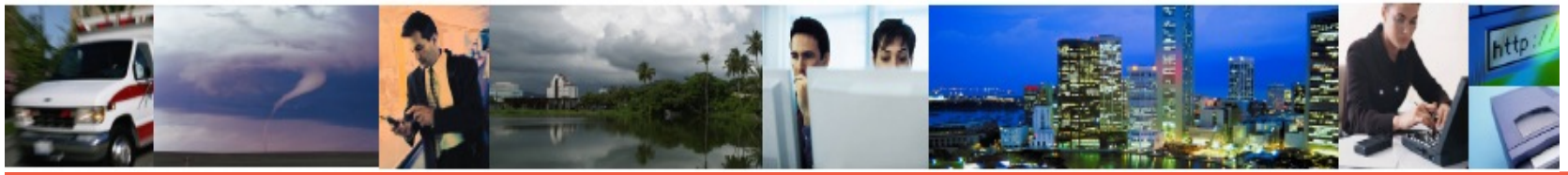
Death by point products

Rising Costs: Do more with less

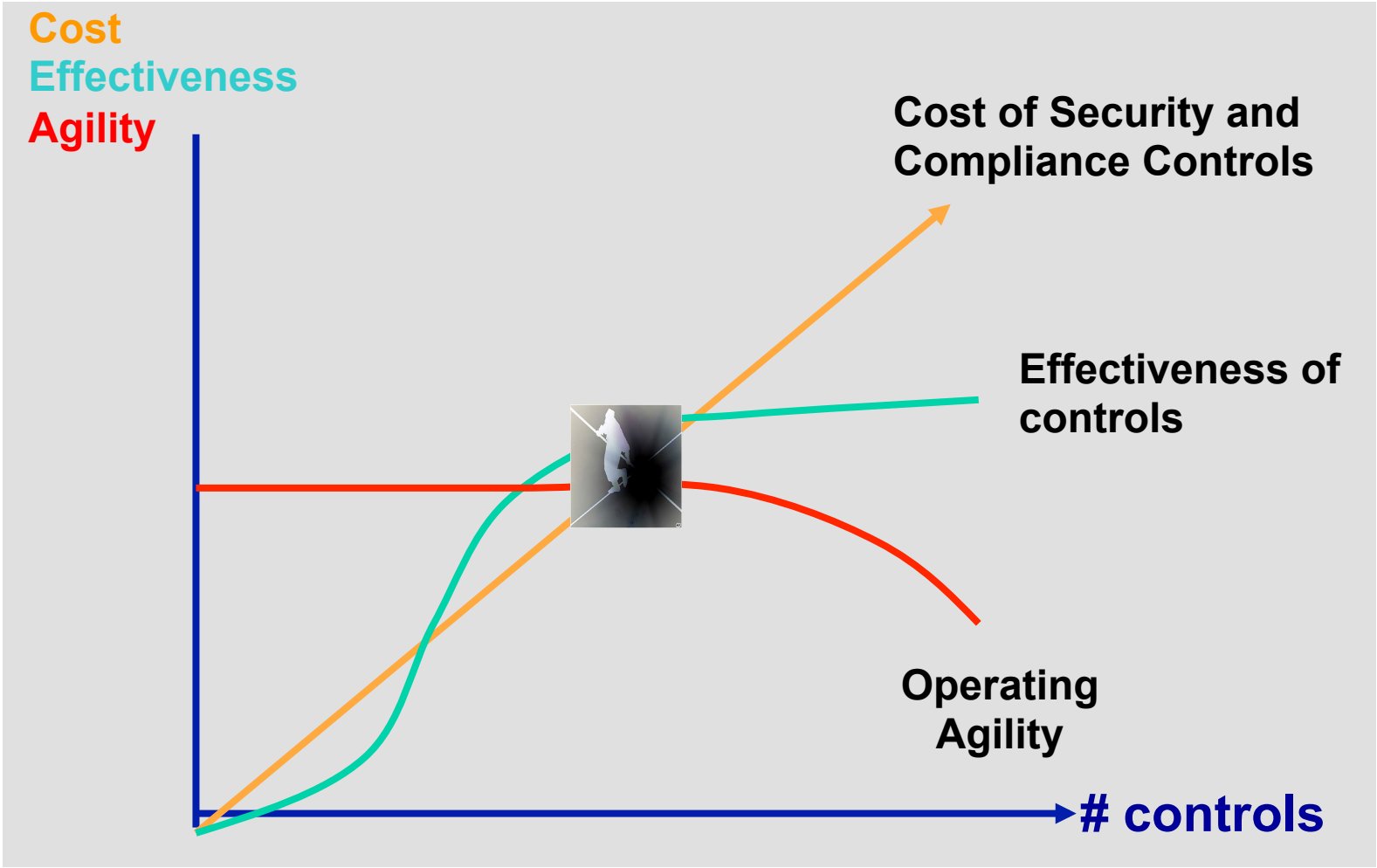
Compliance fatigue

People are becoming more and more reliant on security

IBM believes that security is progressively viewed as every individual's right



Stepping back and re-assessing where you are
The Challenge: Balancing agility, cost, and effectiveness

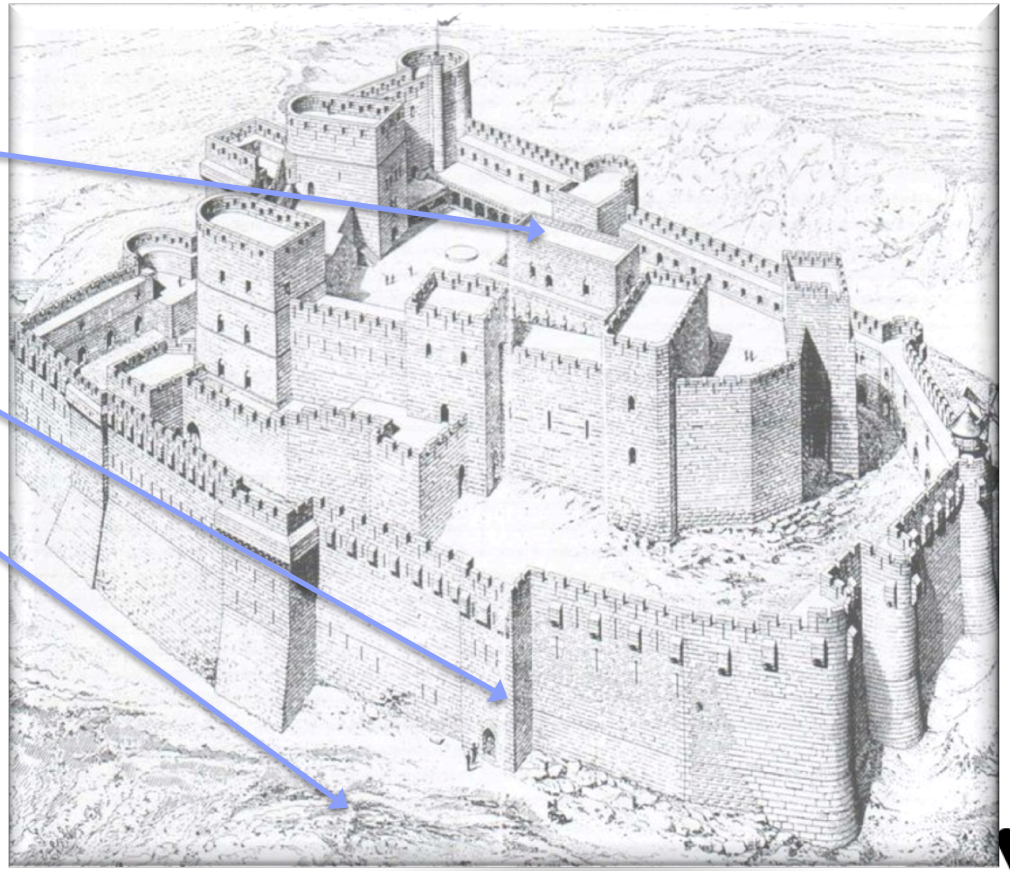


Old Reliable: Defence in Depth Strategy for Privacy and Security

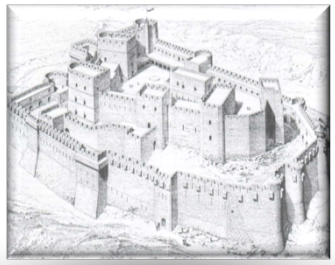
User access monitoring

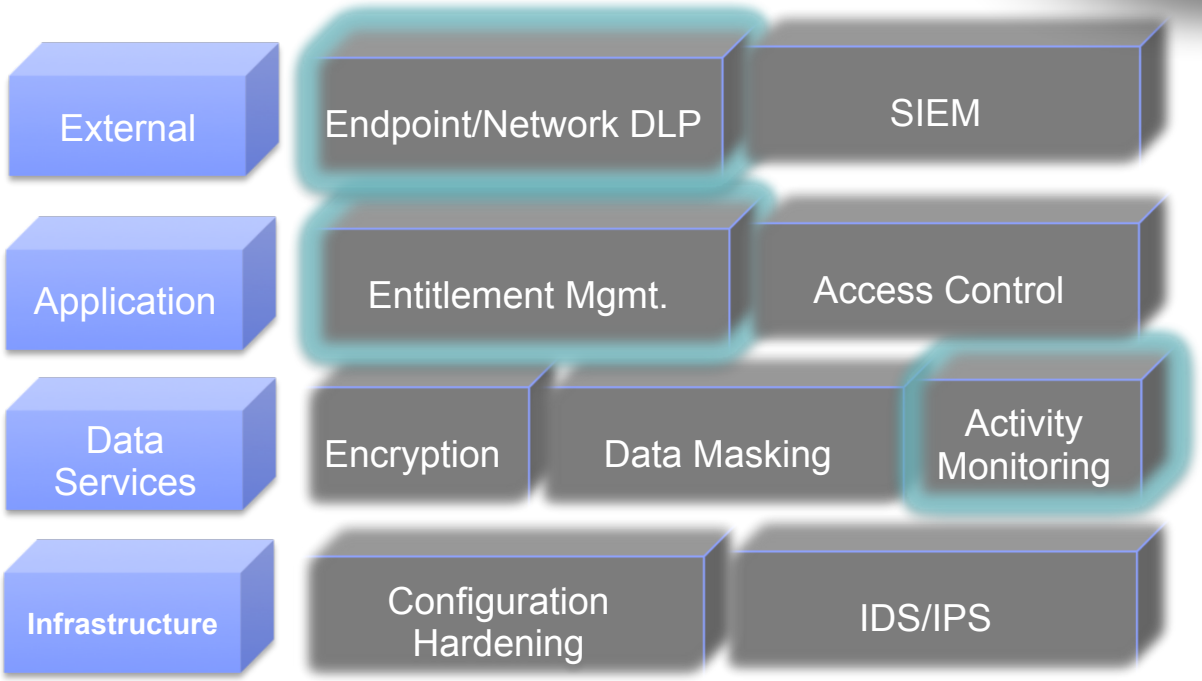
Prevention of unauthorized access

Archiving and retention compliance



Single Security Solutions alone are lacking

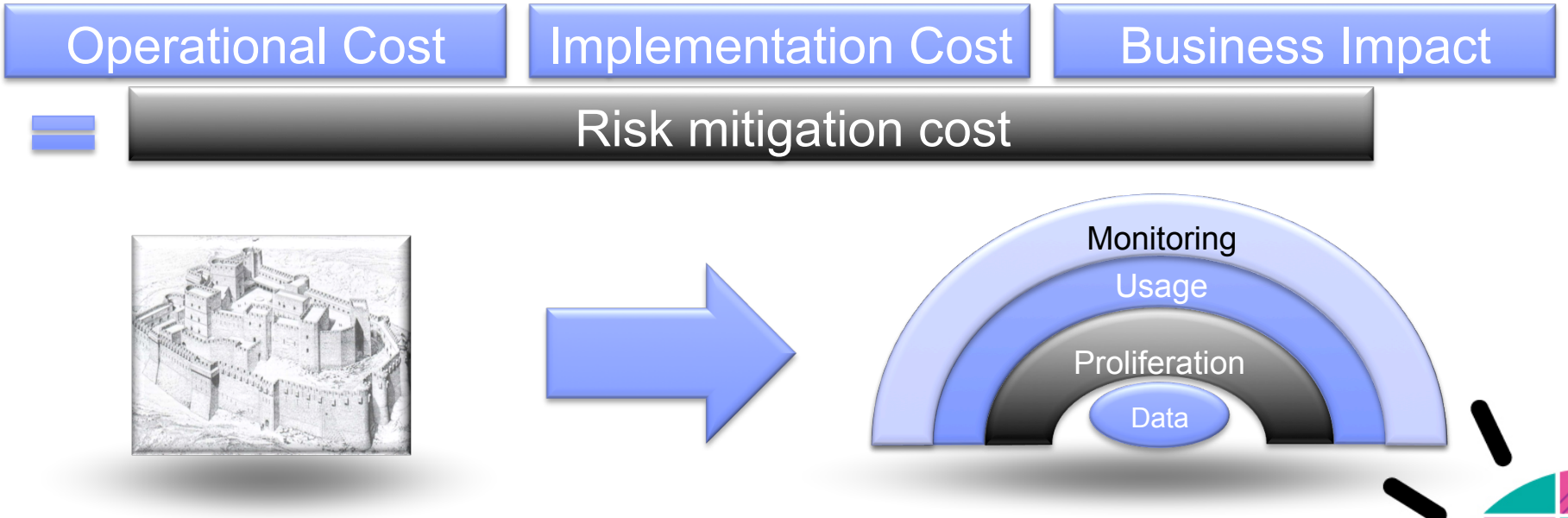




Security is moving toward a risk reduction strategy

Visibility into Risk Costs Money:

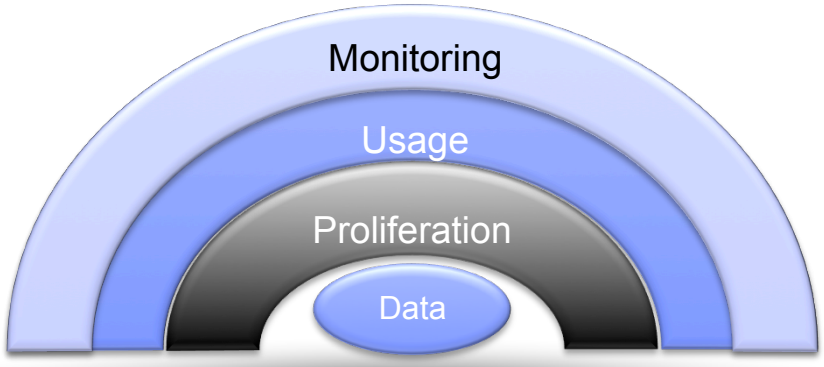
- Funding disparate programs can result in channel conflict
- The lack of applying monitoring controls can result in an underestimated level of risk
- No Security control protects you 100% Represent the risk, not the assurance of protection
- Evaluate the total cost of Control introduction at the business level:



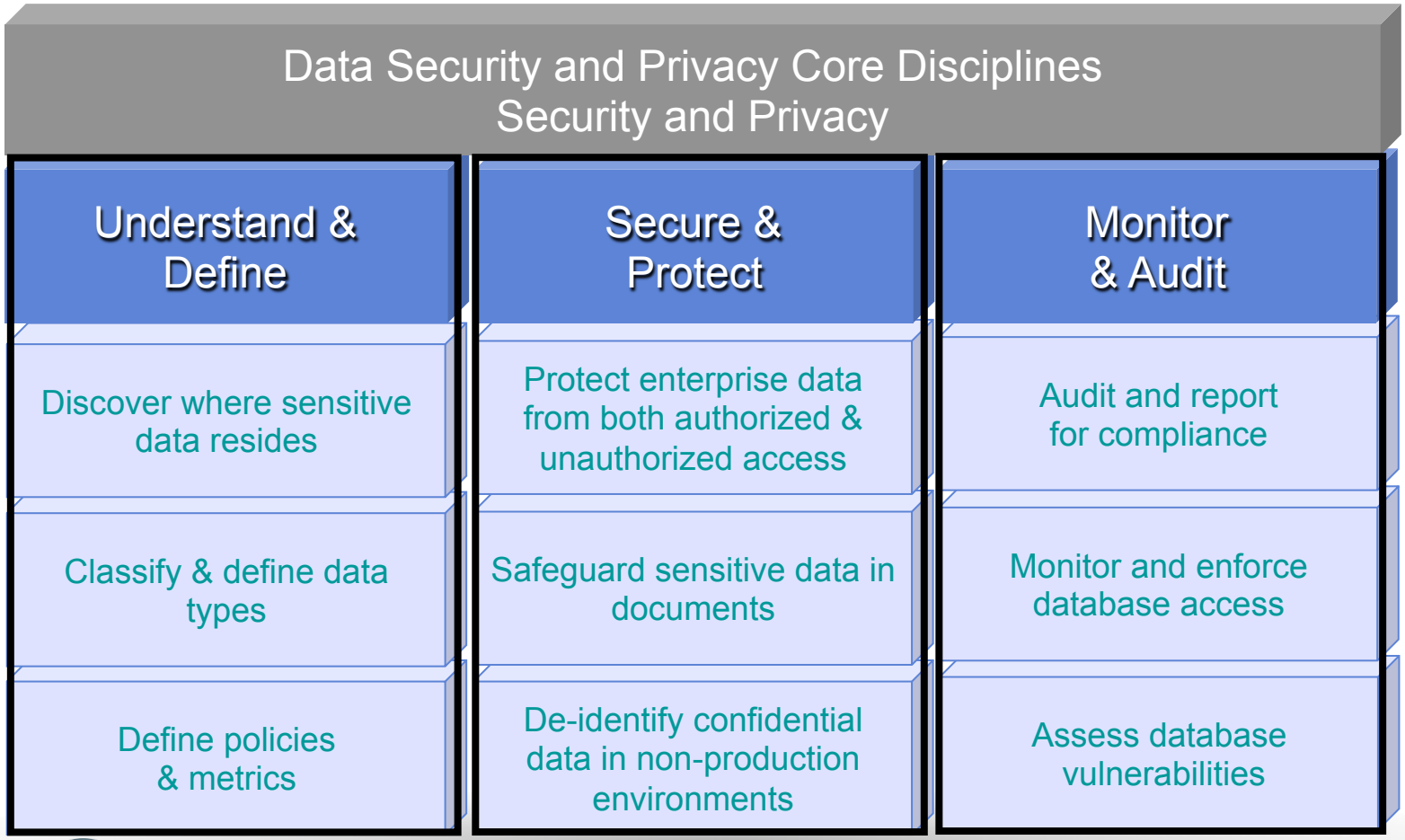
Data security risk reduction strategy

Areas of Consideration:

- **Residence and storage:** *How are you storing your data? Do you know where?*
- **Data Usage:** *Who is using your data? In what systems and applications?*
- **Data Proliferation:** *How fast is your sensitive data being spread across your business?*
- **Behavioral Awareness and Control Efficacy:** *How effective are your controls? How are your measuring their effect?*
- **Evolution:** *From Security implementation to Risk Reduction Strategy*



Where do we see leading organizations heading?



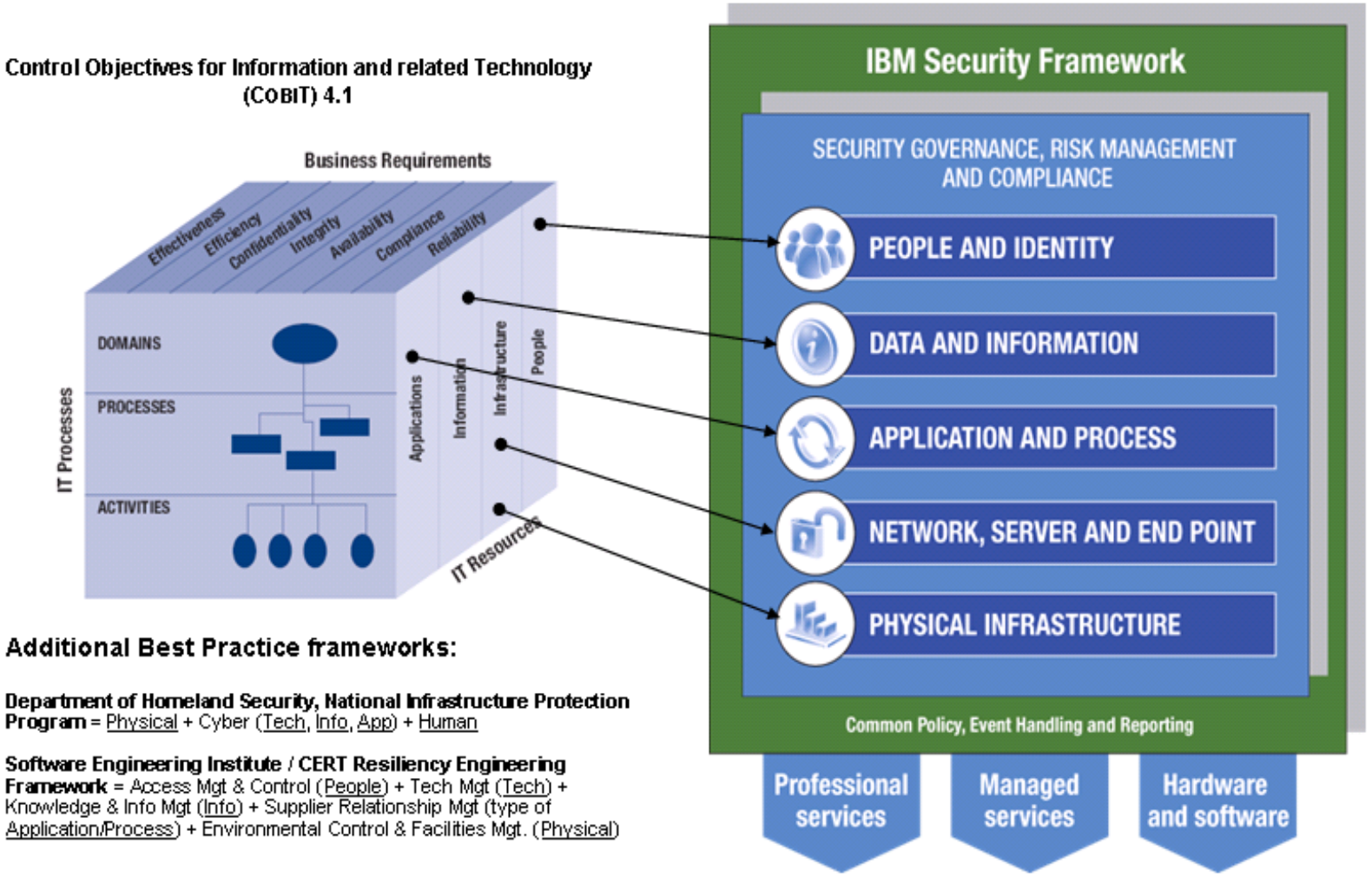
Data Stewards "I need to understand my data better to determine what needs to be secured."

Chief Compliance Officer "We need to ensure we pass all our audits and can prove that privileged users have proper authorizations & data."

Chief Security Officer "I need to ensure we can detect a potential breach before it occurs."

"I need common security policies for my enterprise."

Our Strategy?: The IBM Security Framework



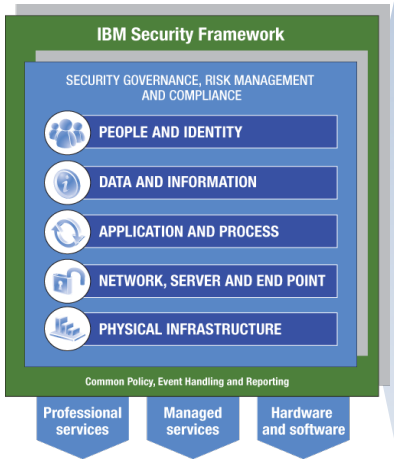
Additional Best Practice frameworks:

Department of Homeland Security, National Infrastructure Protection Program = Physical + Cyber (Tech, Info, App) + Human

Software Engineering Institute / CERT Resiliency Engineering Framework = Access Mgt & Control (People) + Tech Mgt (Tech) + Knowledge & Info Mgt (Info) + Supplier Relationship Mgt (type of Application/Process) + Environmental Control & Facilities Mgt. (Physical)

IBM Security Solutions

- Professional Services
- Managed Services
- Products
- Cloud Delivered



GRC

- Security Governance, Risk and Compliance
- Security Information and Event Management (SIEM) & Log Management

- Identity & Access Management
- Identity Management
- Access Management

- Data Security
- Data Loss Prevention
- Data Entitlement Managment
- Encryption & Key Lifecycle Management
- Messaging Security
- E-mail Security
- Database Monitoring & Protection
- Data Masking

- Application Security
- Application Vulnerability Scanning
- Web Application Firewall
- Web / URL Filtering
- Access & Entitlement Management
- SOA Security

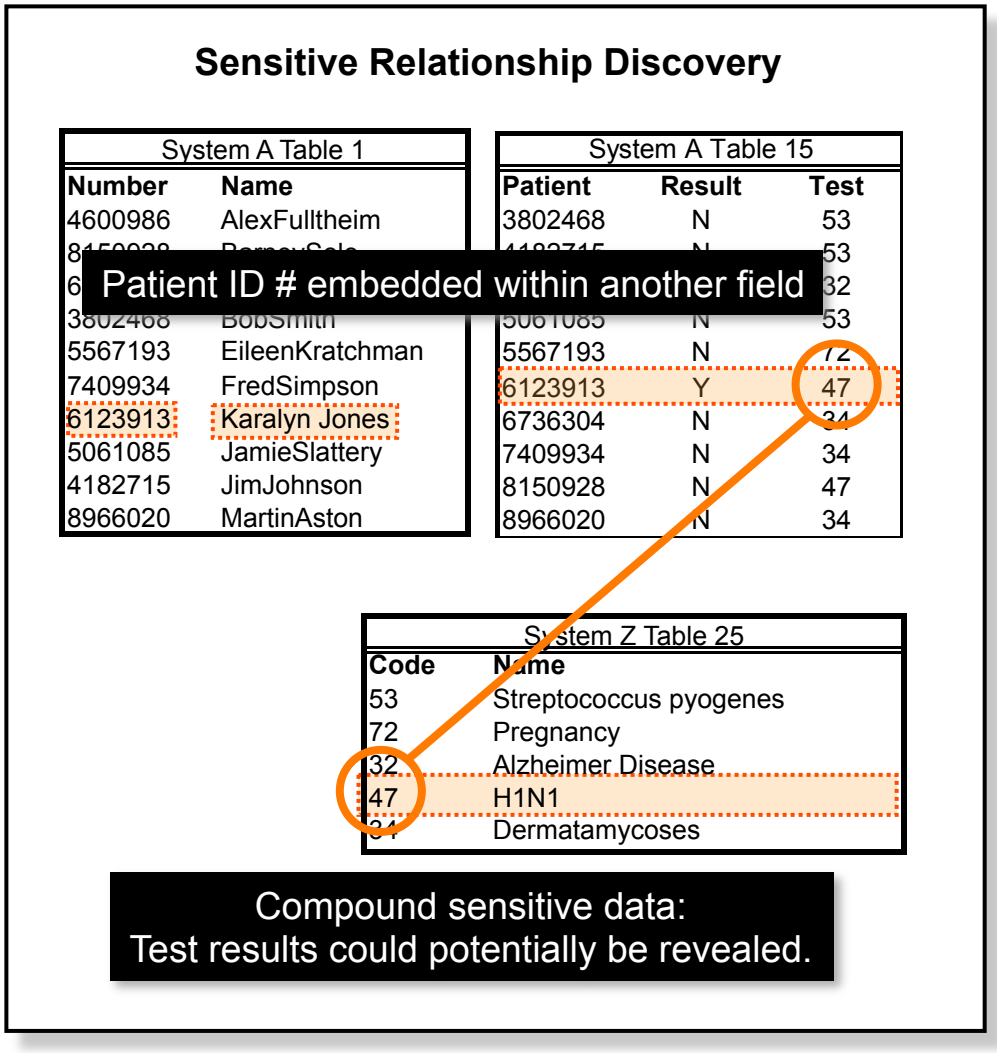
- Infrastructure Security
- Vulnerability Assessment
- Virtual System Security
- Endpoint Protection
- Threat Analysis
- Security Event Management
- Managed Mobility Svcs
- Intrusion Prevention System
- Firewall, IDS/IPS MFS Management
- Mainframe Security Audit, Admin & Compliance
- Security Configuration & Patch Management

- Physical Security

Leading organisations are starting with an understanding of where sensitive data exists

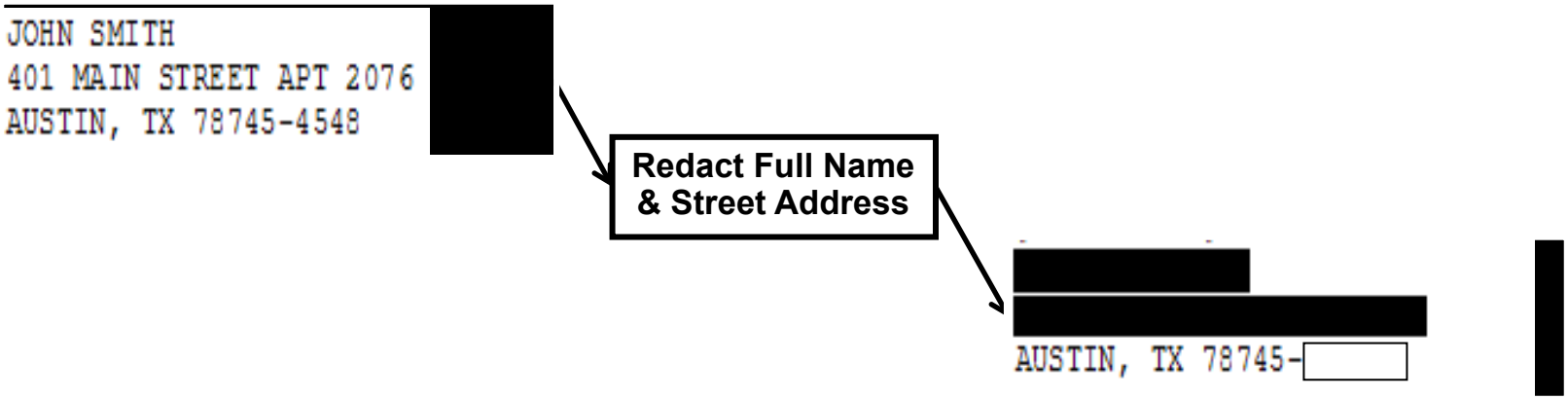
- **Residence and storage**
  - Identifying and managing data, how it is stored, how it is used is a key first step in ensuring ongoing compliance with data security requirements.
  - The more aligned to the business needs the data is, and the better the picture of how and where it is stored, the lower the TCO for security controls will be.
  - Identifying where your sensitive information is and how it is being used informs the strategy of control implementation, and creates a platform for ongoing risk reduction and ensured compliance. Discovery of information is key.
  - Improving security at the storage level (encrypt)

Discover where sensitive data may be hidden



- Relationships and sensitive data can't always be found just by a simple data scan
  - Sensitive data can be embedded within a field
  - Sensitive data could be revealed through relationships across fields & systems
- When dealing with hundreds of tables and millions of rows, this search is complex – you need the right solution

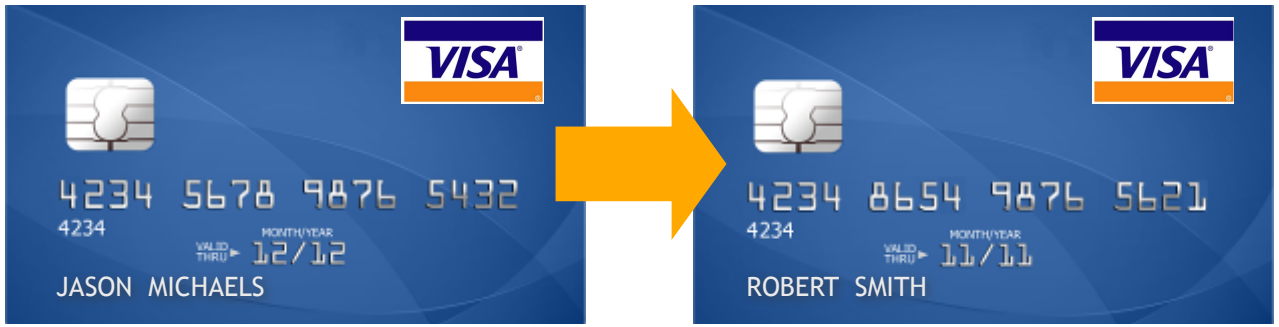
Protect sensitive data values within documents



- Redact (or remove) sensitive unstructured data found in documents and forms, protecting confidential information while supporting the need to share critical business information
- Leverage an automated redaction process for speed, accuracy and efficiency
- Prevent unintentional disclosure by using role-based masking to confidently share data
- Ensure multiple file formats are supported, including PDF, text, TIFF and Microsoft Word documents

De-identify data without impacting test and development

- Mask or de-identify sensitive data elements that could be used to identify an individual
- Ensure masked data is contextually appropriate to the data it replaced, so as not to impede testing
- Support referential integrity of the masked data elements to prevent errors in testing

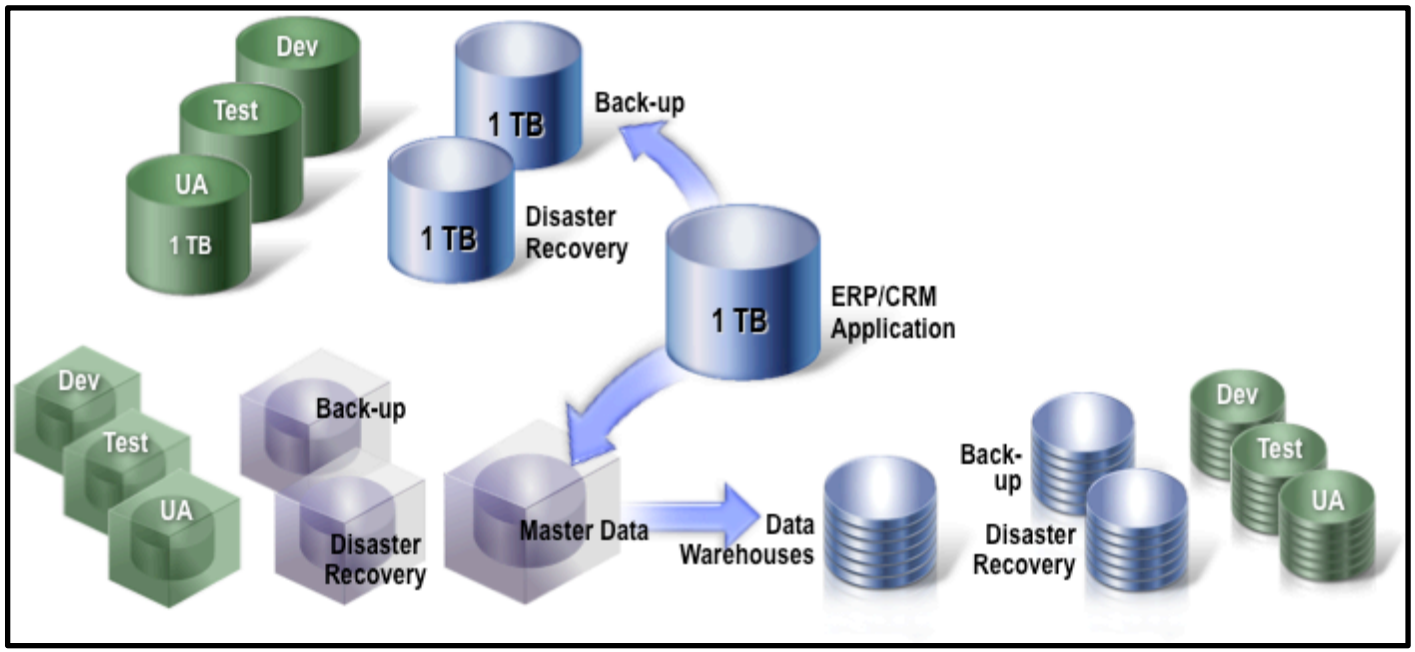


Personal identifiable information is masked with realistic but fictional data for testing & development purposes.

Proliferation – Determining how to reduce the "Attack Landscape"

Instituting a standard of usage:

- Providing tools to manage the use of data during the development or implementation cycle prevents the seeds of non-compliant behavior.
- Non-production data systems represent a significant source of data proliferation and can ultimately be the source of many instances of circumvented controls that lead to non-compliance and eventually a higher risk of breach.



Database activity monitoring

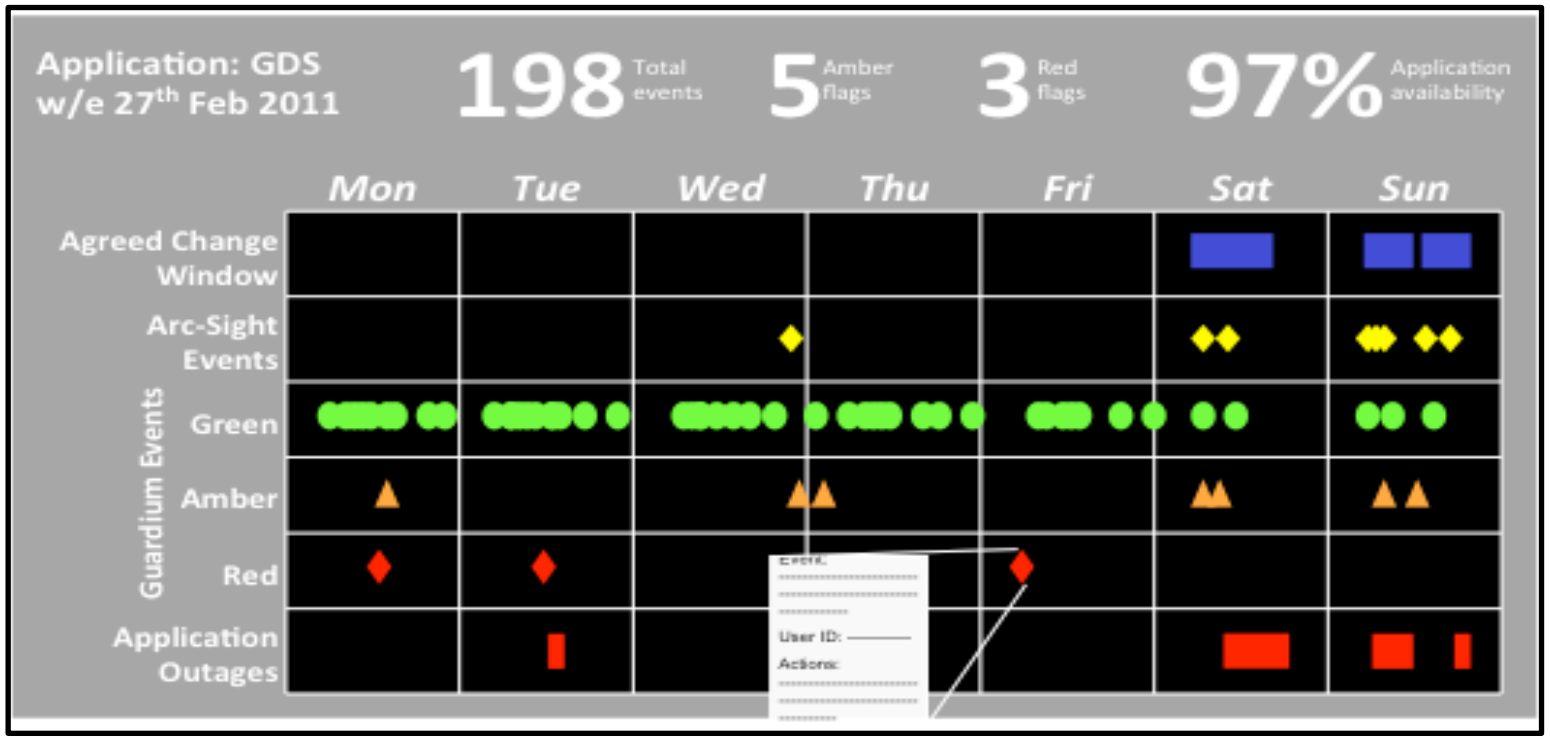
Real-time database security & compliance

Benefits Summary

- Protect against data breaches & fraud
- Prevent unauthorized changes to critical enterprise data (SAP, PeopleSoft, etc.)
- Reduce compliance costs through automated, centralized & standardized controls
- SQL injection protection

Behavioral Awareness and Control Efficacy

– Monitoring at the data level gives the business insight into appropriate and inappropriate usage of data, informing and prioritizing strategy.
– Understanding and creating awareness at a risk level and at a business level creates the opportunity to best guide not only technology, but also awareness and business practices.



Streamline and simplify compliance processes

- Alerts of suspicious activity
- Audit reporting and sign-offs
- Separation of duties – creation of policies vs. reporting on application of policies
- Trace users between applications, databases
- Fine grained-policies
- Sign-off and escalation procedures
- Integration with enterprise security systems (SIEM)

Protecting data is both an external and internal issue

- Prevent “power users” from abusing their access to sensitive data (separation of duties)
- Prevent authorized users from misusing sensitive data
- Prevent intrusion and theft of data
- Prevent inappropriate “re-location of data via portable devices” (DVD/USB/Mobile Phones)

Protection of data requires a 360-degree strategy

- Secure structured and unstructured sensitive data values
- De-identify data
- Stop unauthorized data access

Security makes it possible for us to take risk, and innovate confidently.

PCI Compliance for McAfee.com

- **Who:** Global security company
- **Need:** Safeguard millions of PCI transactions
  - Maintain strict SLAs with ISP customers (Comcast, COX, etc.)
  - Automate PCI controls
- **Environment:** Guardium deployed in less than 48 hours
  - Multiple data centers; clustered databases
  - Integrated with ArcSight SIEM
  - Expanding coverage to SAP systems for SOX
- **Previous Solution:** Central database audit repository with native DBMS logs
  - Massive data volumes; performance & reliability issues
  - Separation of Duties (SOD) issues
- **Results**
  - *"McAfee needed a solution with continuous real-time visibility into all sensitive cardholder data – in order to quickly spot unauthorized activity and comply with PCI-DSS – but given our significant transaction volumes, performance and reliability considerations were crucial."*

Securing SAP & Siebel: 239% ROI and <6 Months Payback

- **Who:** F500 consumer food manufacturer ($15B revenue)
- **Need:** Secure SAP & Siebel data for SOX
  - Enforce change controls & implement consistent auditing across platforms
- **Environment**
  - SAP, Siebel, Manugistics, IT2 + 21 other Key Financial Systems (KFS)
  - Oracle & IBM DB2 on AIX; SQL Server on Windows
- **Results: 239% ROI & 5.9 months payback, plus:**
  - **Proactive security:** Real-time alert when changes made to critical tables
  - **Simplified compliance**: Passed 4 audits (internal & external)

    "The ability to associate changes with a ticket number makes our job a lot easier … which is something the auditors ask about." [Lead Security Analyst]
  - **Strategic focus on data security**

    "There's a new and sharper focus on database security within the IT organization. Security is more top-of-mind among IT operations people and other staff such as developers."

Commissioned Forrester Consulting Case Study

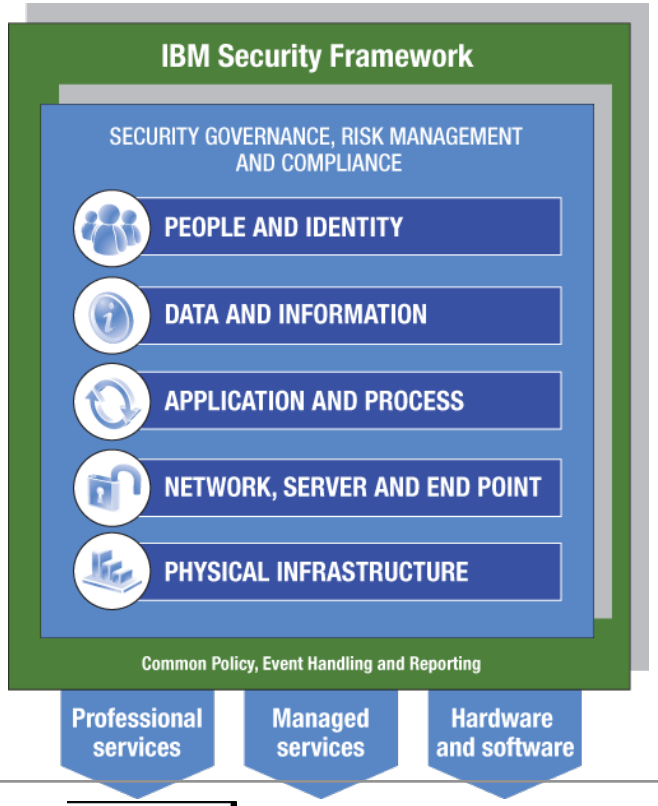
Safeguarding Customer Information for Washington Metropolitan Area Transit Authority (Metro)

- **Who:** Operates 2nd largest U.S. rail transit system and transports more than a third of the federal government to work
- **Need:** Metro needed to safeguard sensitive customer data and simplify compliance with PCI-DSS -- without impacting performance or changing database configurations
  - Protecting customer data
  - Passing audits more quickly and easily
  - Monitoring for potential fraud in PeopleSoft system
- **Environment**
  - More than 9 million transactions per year (Level 1 merchant)
  - Complex, multi-tier heterogeneous environment

- **Alternatives considered:** Native logging and auditing impractical
- **Customer Impact:** "Our customers trust us to transport them safely and safeguard their personal information."
  - "We looked at native DBMS logging and auditing, but it's impractical because of its high overhead, especially when you're capturing every SELECT in a high-volume environment like ours. In addition, native auditing doesn't enforce separation of duties or prevent unauthorized access by privileged insiders."

IBM Security Solutions provide a holistic approach which can allow you to securely, safely, and confidently adopt new forms of technology

- The ***only 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 and risk management patents
- **200+** security customer references and 50+ published case studies
- **40+** years of proven success securing the zSeries environment
- **600+** security certified employees (CISSP,CISM,CISA,..)

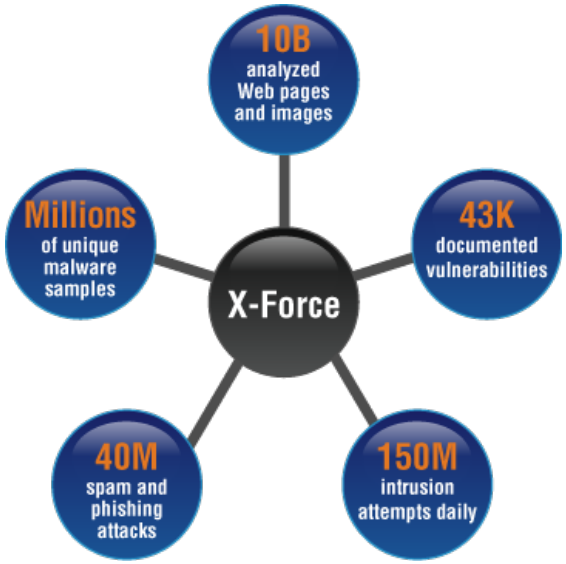


Security Acquisitions:

DASCOM, consul an IBM company, watchfire, Guardium, INTERNET SECURITY SYSTEMS, BIGFIX An IBM Company, access360 A Better Way To Manage Access Rights, ENCENTUATE An IBM Company, OUNCE LABS an IBM company, princeton softech an IBM Company, INTELLIDEN, OPENPAGES, Initiate, DATAPOWER

Why IBM? – Leaders in their field

IBM researches and monitors latest threat trends with X-Force



Provides Specific Analysis of:

- Vulnerabilities and exploits
- Malicious/Unwanted websites
- Spam and phishing
- Malware
- Other emerging trends

Most comprehensive vulnerability database in the world

- Entries date back to the 1990's

Source: IBM X-Force Database, www.ibm.com/federal/security

IBM is dedicated to cybersecurity advancement

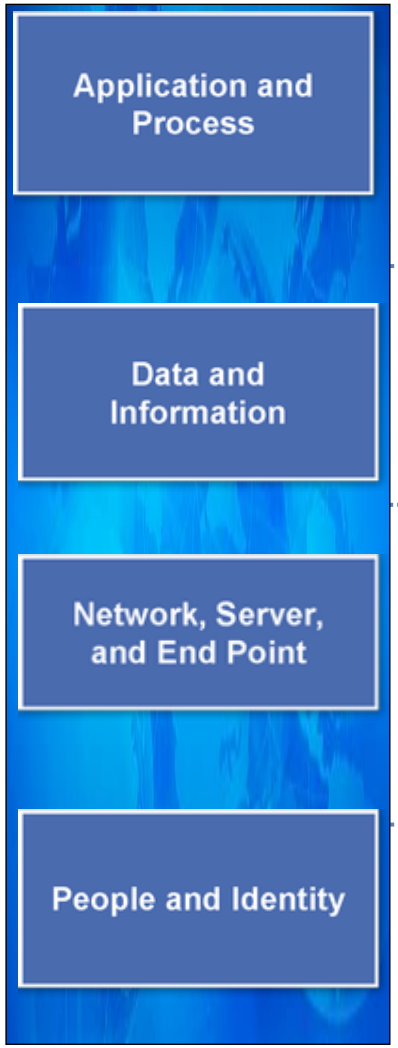
Institute Focus

- **Engage** in public-private collaboration
- **Address** and mitigate cybersecurity challenges
- **Provide** a forum for clients to better understand how recent IBM Research advances can help

http://www.instituteforadvancedsecurity.com/

X-Force Trend Report
Attacks Continue Across all Security Domains

IBM X-Force® 2010 Trend and Risk Report
March 2011



- 2010 saw the largest number of vulnerability disclosures in history, up **27%**. This increase has had a significant operational impact for anyone managing large IT infrastructures. More vulnerability disclosures can mean more time patching and remediating vulnerable systems.
- **49%** of the vulnerabilities disclosed in 2010 were web application vulnerabilities.
- **44%** of all vulnerabilities disclosed had no vendor-supplied patches available at the end of 2010.

- Bot network activity continued to grow in 2010. Consolidation among Trojan botnets is expected to be an emerging trend.
- The term "Advanced Persistent Threat" became an everyday part of the corporate security lexicon after high profile attacks on corporate enterprises by sophisticated, targeted attackers.
- Anonymous proxy websites continue to increase in volume, quintupling since 2007.

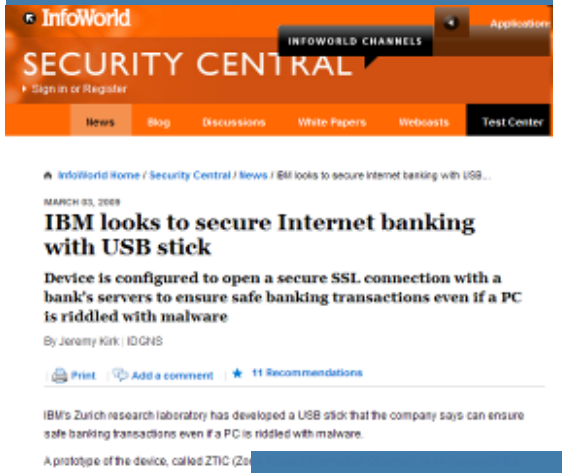
- The SQL Slammer worm first surfaced in January 2003 and became known as one of the most devastating Internet threats of the past decade. This worm continued to generate a great deal of traffic on the Internet in 2010.
- Obfuscation, whereby attackers attempt to hide their activities and disguise their programming, continued to increase over 2010 and shows no signs of waning.
- SQL injection is one of the leading attack vectors seen in 2010 because of its simplicity to execute and its scalability to compromise large amounts of Web servers across the Internet.

- USA, India, Brazil, Vietnam, and Russia are the top five countries for spam origination in 2010.
- The vast majority of spam, more than **90%**, is still classified as URL spam.
- The amount of URL spam using well-known and trusted domain names declined slightly in the 2nd half of 2010, for the first time in more than two years.
- The top spam domains have moved from China (.cn) to Russia (.ru).
- In 2010, financial institutions continue to climb as the number one target for phishing attempts, representing **50%** of the targeted industries.

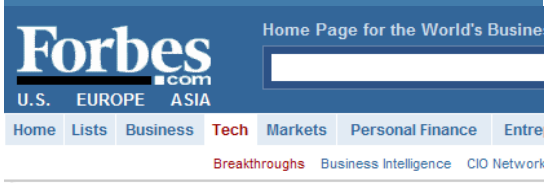
A visionary in the field of IT Security… highlights of recent IBM security Research projects

Trusted Virtual Data Center, and Security Svcs. in Virtualized Environments

Cryptography and Security Research



Cryptography Research



MetaData

IBM's Plans for Nimbler Encryption

Andy Greenberg, 06.24.09, 07:00 PM EDT

The computing giant has big plans for its new encryption algorithm.

Craig Gentry has made a huge
It may be a decade before
pe to practically implement Gentry's
n, but IBM is already planning
mix of privacy and computation.

Identity Governance

IBM wins European Identity Award

Makes Available New Open Source Code for Developing Privacy-Friendly ID Management Applications

Top story

English | German

Munich, Germany, 5 May 2010—IBM Research was honored with the Best Innovation European Identity Award 2010 from Kuppinger Cole, an analyst firm focused on information security, identity, and IT governance. IBM's Identity Mixer technology was recognized for its pioneering work that offers simultaneously both strong authentication and privacy. The award will be presented this evening at the firm's annual European Identity Conference in Munich. Simultaneously, IBM Research is also announcing that the latest version of its IBM Identity Mixer technology is now available free-of-charge.

Secure software and services

Case Studies

- **Data Privacy in Telecommunications**
- http://www-01.ibm.com/software/success/cssdb.nsf/CS/JHAL-8DMTGN?OpenDocument&Site=software&cty=en_us

- **Data Security and Compliance in Healthcare**
- http://www-01.ibm.com/software/success/cssdb.nsf/CS/JHAL-8DMUU6?OpenDocument&Site=software&cty=en_us

Thank You


cám
asko
formal
mercé
kiitos
maita
mersi
akpé
dankon
deu
nanni
thank
mèsi
beacôp
Allahu
khob
chnorakaloutioun
leat
milesker
bedankt
dank
terima
dakujem
sana
diakuju
obrigado
po
pa
dziękuję
go
grazie
krap
najis
ederim
pers
mamnun
leibh
edirem
shukriya
tesekkur
mochchakkeram
enkosi
faafetai
didi
kyay
gratias
nirringrazzjak
arigatô
gracias
graciñas
kha
aabhar
much
sag
ago
hamnida
grâces
grazzi
bayarlalaa
blagodaram
dhanyavaad
dhanyabaa
merci
dankie
danke
sobodi
akun
gràcie
dankewol
ngiyabonga
dziakuju
ko
ačiū
ni
je
tapadh
chai
kop
salamat
misaotra
meharbani
gratzias
familiar
ju
aguyjé
plural
kasih
kié
vala
fyri
nandri
murakoze
khun
takk
obrigada
täna
saha
agat
raibh
kam
asante
lava
paldies
köszönöm
chokrane
dieuf
děkuji
marahaba
efharisto
barkal
northern
djiere
eskerrik
fiik
motashakkeram
danki
côps
basque
mulţumesc
dhanyavadagalu
Barak
maith