IBM SECURITY DAY 2011

Innovare con sicurezza per aprire al futuro

Tiziano Airoldi

La Sicurezza dei Dati Aziendali

Data Security … a top priority for any company

Data Security …. a **complex** and **difficult** task

Strategic for the business and **vital** for the company

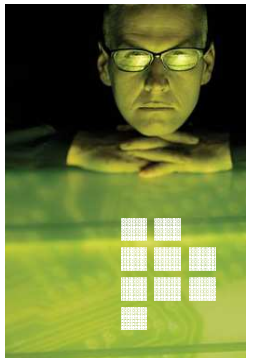
why ?

new business strategies

virtualization, cloud computing, mobile computing

collaboration, social networks, the Internet of things

and the information explosion !

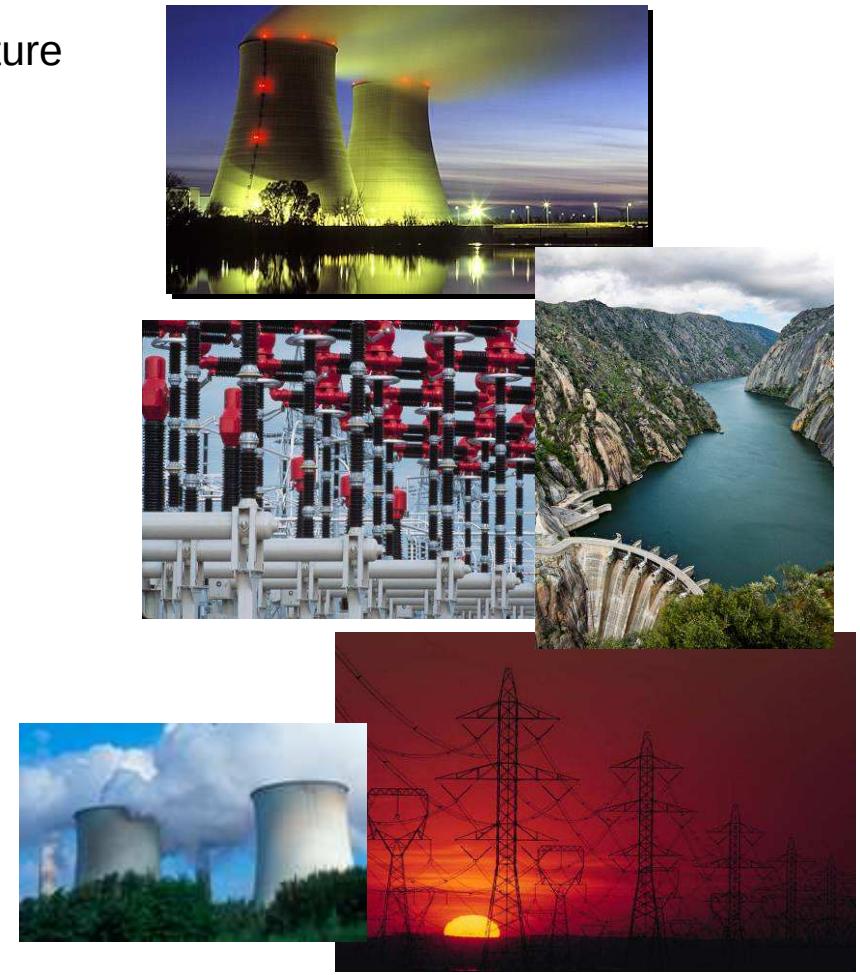


Data Security: a pain point for any industry sector

- Money has become intangible, invisible. It's information
- Keeping up with regulatory and maintain compliance posture (PCI DSS, SOX, Basel II & III, Privacy Law, HIPAA, Solvency…)
- Protect security and privacy of critical information
- Personal Information privacy protection (PII)
- Data breaches and related costs
- Insider threat and Fraud
- Identity theft
- SCADA Information Security
- Data Integrity and Transaction Integrity

Impact of a Data Breach to Power Control Systems could be severe

- Serious disruption to national critical infrastructure
- Loss of system availability
- Process interruption
- Equipment damage
- Asset mis-configuration
- Loss of data and confidentiality
- Personal injury
- Penalties resulting from regulatory violations
- Loss of customer and public trust



Impact of a Information Security Incident to Financial Institutions could be severe

- Increased risk of fraud and other criminal activity
- Increased threats from disgruntled employees
- Virtualization and cloud computing increase infrastructure complexity
- Mobile platforms are developing as new means of identification
- Data volumes are doubling every 18 months
- Storage, security and discovery around information context is critical
- The vast majority of clients are having issues with disclosing sensitive business data to the wrong people
- Significant costs associated with a data breach

The main issues for information security in the Public Sector

- Protect Security and Privacy of critical assets (logical/physical) has never been more critical
- Government organizations, suppliers, vendors all need to be certain that confidential data is protected from internal and external threats
- Meet ever evolving regulatory compliance requirements
- A breach of organizational network, systems or data could result in financial and legal impact as well as impact on an organization's reputation
- Hackers and data thieves are well organized, well funded and their activities are accelerating

Data Lifecycle

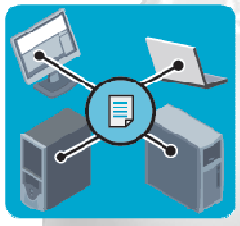
8:00AM

The **director** of finance **downloads** data from the customer database. He drafts the “Year End” results spreadsheet and **saves** it on his **desktop** PC.

Data Lifecycle

10:00AM

The **director** stores a copy of “Year End” results in a **shared directory** on a corporate **server** for the finance team.



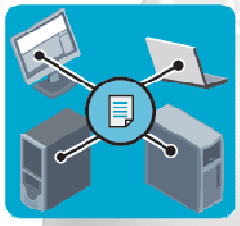
The **director** of finance **downloads** data from the customer database. He drafts the “Year End” results spreadsheet and **saves** it on his **desktop** PC.

Data Lifecycle

12:30PM

The finance **manager** accesses the “Year End” results, adjusts the numbers, and **emails** the file to the company’s **outside accountant**.

The **director** stores a copy of “Year End” results in a **shared directory** on a corporate **server** for the finance team.



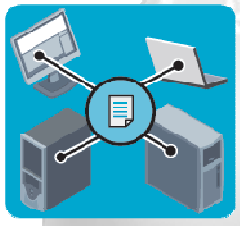
The **director** of finance **downloads** data from the customer database. He drafts the “Year End” results spreadsheet and **saves** it on his **desktop** PC.

Data Lifecycle

3:00PM

The finance **manager** accesses the “Year End“ results, adjusts the numbers, and **emails** the file to the company’s **outside accountant**.

The **director** stores a copy of “Year End” results in a **shared directory** on a corporate **server** for the finance team.



The **accountant** accesses the email on a **handheld** and **forwards** it with comments to a **colleague**. She reviews “Year End” results and **saves** it on a **laptop** and a **thumb drive**.

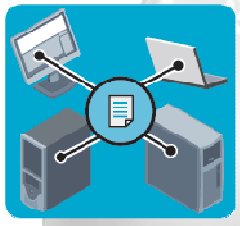
The **director** of finance **downloads** data from the customer database. He drafts the “Year End” results spreadsheet and **saves** it on his **desktop** PC.

Data Lifecycle

5:30PM

The finance **manager** accesses the "Year End" results, adjusts the numbers, and **emails** the file to the company's **outside accountant**.

The **director** stores a copy of "Year End" results in a **shared directory** on a corporate **server** for the finance team.



The **accountant** accesses the email on a **handheld** and **forwards** it with comments to a **colleague**. She reviews "Year End" results and **saves** it on a **laptop** and a **thumb drive**.

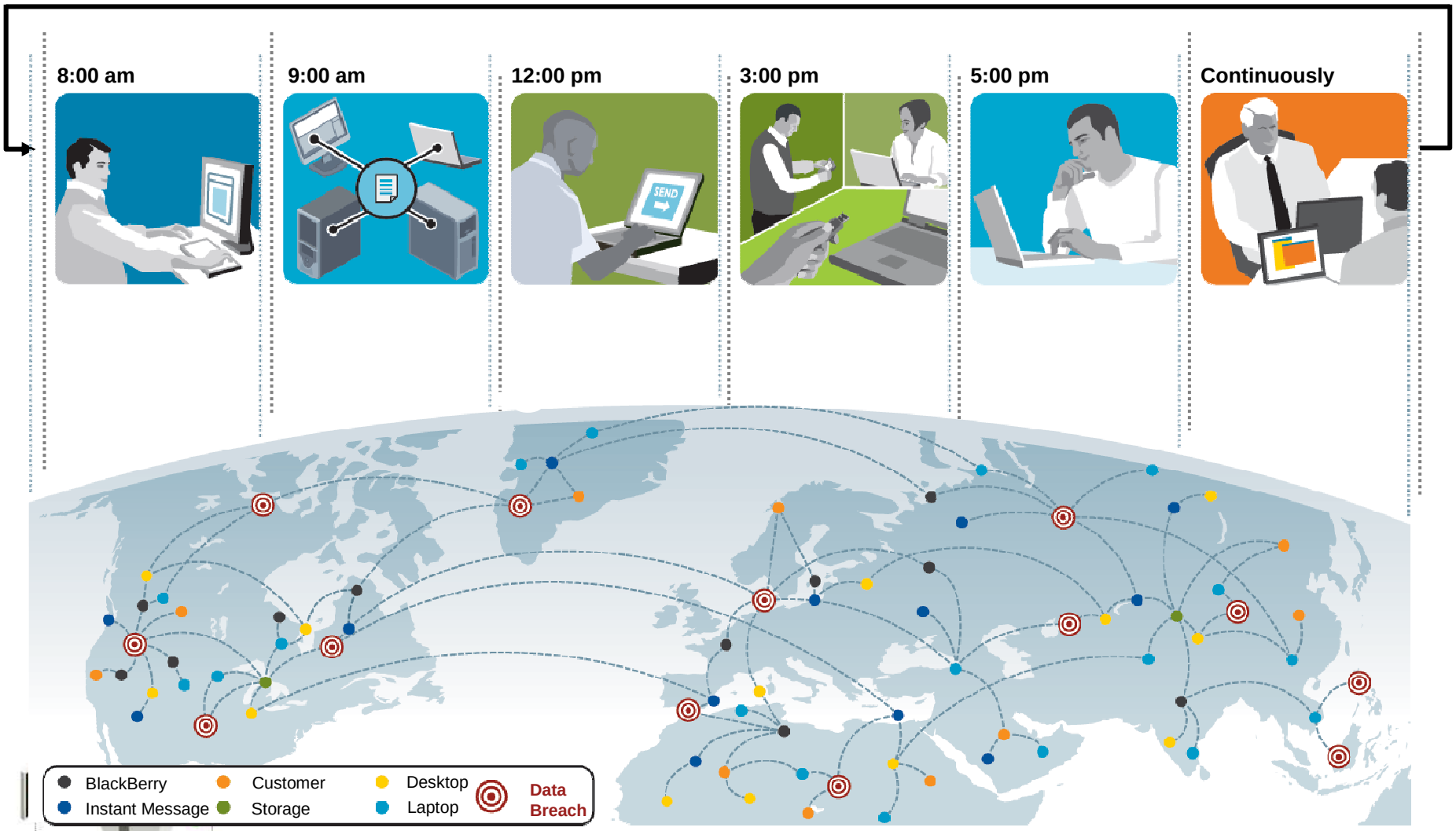
The **director** of finance **downloads** data from the customer database. He drafts the "Year End" results spreadsheet and **saves** it on his **desktop** PC.

The **colleague** gives the thumb drive to the **onsite auditor**, who **transfers** "Year End" results to his **laptop** so he can review it later at **home**.

Data Lifecycle .... the underpinning risks

- How many places was the data stored today ?
  - **Customer Database**
  - Director of Finance's PC
  - Corporate Server
  - Company's Email Server
  - Outside Accountant's Email Server
  - Outside Accountant's Handheld Email
  - Colleague's Email
  - Colleague's Laptop
  - Colleague's Thumb Drive
  - Auditor's Laptop

Data Lifecycle: Multiple Threats



The Risk of Data Leakage

Confidential Data Types

Customer Data
Social Security Numbers
Credit Card Numbers
Protected Health Info

Corporate Data
Financials
Mergers and Acquisitions
Employee Data

Intellectual Property
Source Code
Design Documents
Pricing

The Risk

1:400 messages contains confidential data

Source: Vontu Risk Assessment findings

1:50 network files is wrongly exposed

Source: Vontu Risk Assessment findings

4:5 companies lost data on **laptops**

Source: Ponemon Institute survey study (August 2006)

1:2 companies lost data on **USB drives**

Source: Forrester Consulting survey (February 2007)

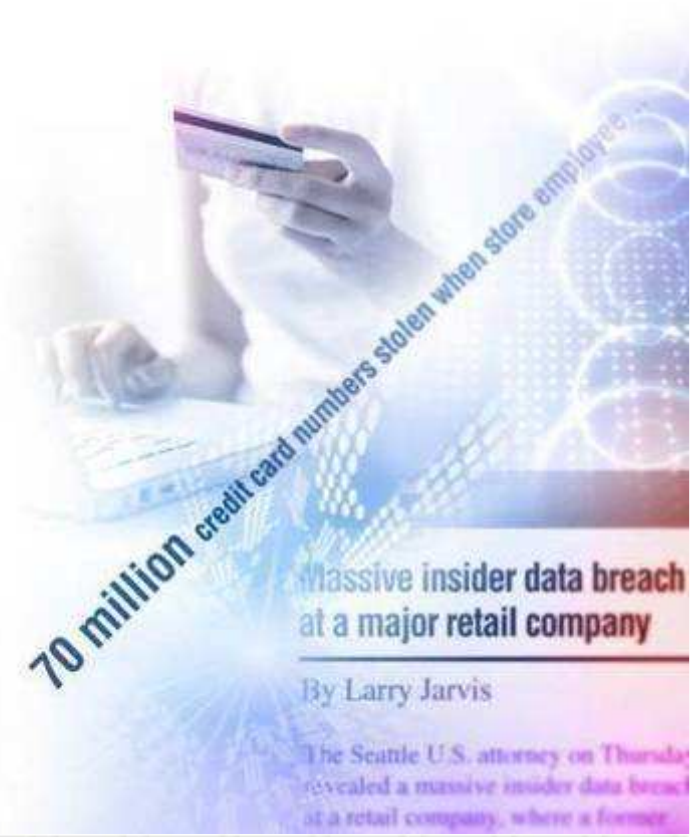
14

The value of the information in the market

"Information is itself the target.
Information is the world's new currency."

— Ralph Basham, Director, United States Secret Service

[1] Ponemon Institute, *2008 Annual Study: Cost of a Data Breach*, Feb 2009.



Data Security is seen by CIO's as the highest priority of security projects

The Drivers:

- **An Information Explosion – data volumes doubling every 18 months**
- **Significant costs associated with a data breach**
  - Ave cost = $202 / record
  - Ave cost = $6.6 M / breach
  - Half of losses due to insider misuse
- **Compliance with regulatory requirements and corporate policies**
- **Proliferation of data protection challenges and vendor tools**

2-1 Data Security And Vulnerability And Threat Management Are Top Priorities

Managing vulnerabilities and threats jumped to the No. 2 spot on the list in 2009, up from No. 6 in 2008

"Which of the following initiatives are likely to be your firm's/organization's top IT security priorities over the next 12 months?"

	Critical priority	High priority	Low priority	Not on our agenda	Don't know/does not apply
Data security	38%	51%	9%		1%
Managing vulnerabilities and threats	31%	54%	13%	1%	1%
Cutting costs and/or increasing efficiency	36%	45%	16%	3%	1%
Business continuity/disaster recovery	30%	48%	19%	2%	1%
Regulatory compliance	36%	41%	17%	5%	1%
Managing information risk	23%	53%	20%	3%	1%
Application security	19%	54%	23%	3%	1%
Aligning IT security with the business	18%	55%	21%	5%	1%
Identity and access management	22%	49%	23%	5%	1%
User security training and awareness	13%	50%	32%	5%	1%
Implementing our security requirements on business partners/third parties	11%	36%	34%	17%	3%
Security outsourcing	11%	39%	45%	2%	2%

Base: 1,009 North American and European enterprise IT security sourcing and services decision-makers (percentages may not total 100 because of rounding)

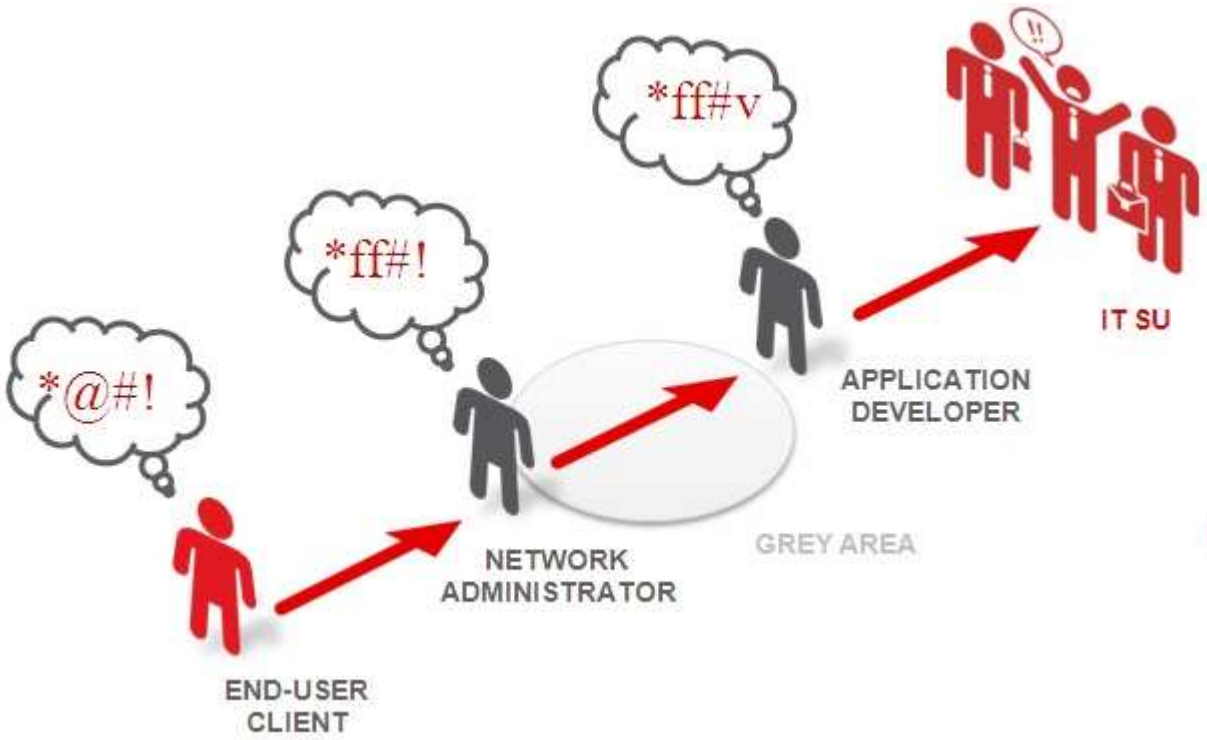
What are the **right questions** for data security ?

- How do you **identify** where your sensitive data resides and how it is used in your business processes ?
- When did you last **assess** how secure your critical data is and where points of data leakage could exist ?
- What is your **strategy** for data protection, and how well is it aligned to your risk management objectives ?
- What industry regulatory **requirements** for protecting data most concern you, and to what extent do you feel you are **compliant** with these regulations today ?
- Who has **privileges** in your organization to access data and how do you enforce and monitor these accesses ?
- Do you know **who's accessing** your data when, how and why ?

What are the **right answers** in data protection ?

*or … what are the **best options** for my organization ?*

Who's responsible ? Who's accountable ?



IT ? or Business ?

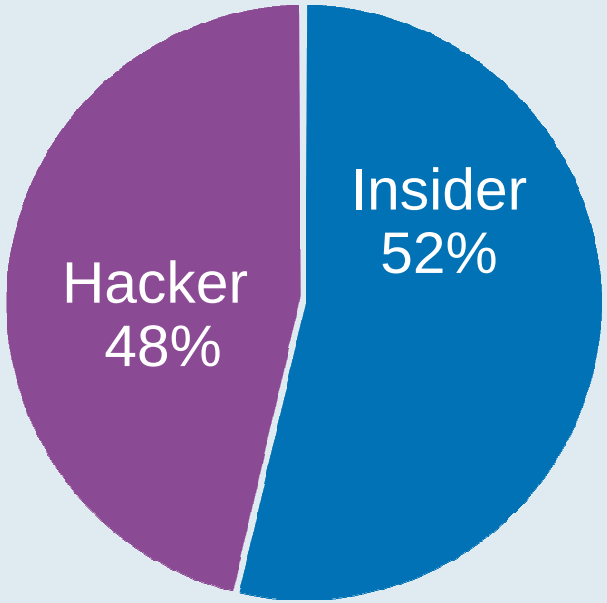
The only secure collaboration is no collaboration or no information exchange ?

Blocking is not always the right answer
Data security is about enhancing collaboration while mitigating risk

The Threat of Data Leakage

Insider vs. The Hacker

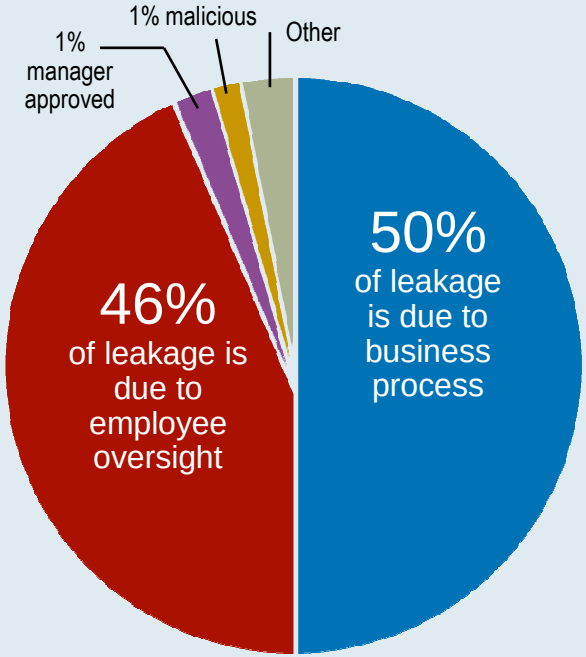
Breaches Since 2005:
230 and Counting
> 93M Records



Data compiled from industry sources including EPIC.org and PerkinsCoie.com

Inadvertent vs. Malicious

96% of leaks are due to faulty processes or oversight



Source: Vontu Risk Assessment findings.

59 percent of individuals who were laid off, fired or quit their jobs in the past 12 months have admitted to stealing company data.

Source: http://www.networkworld.com/news/2009/022309-fired-workers-steal-data.html

21

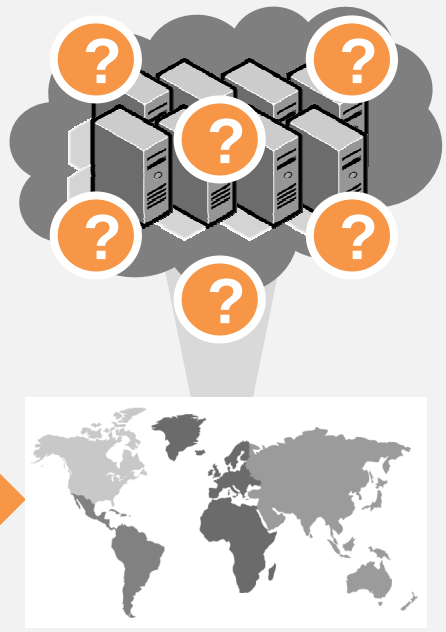
Virtualization and cloud makes it harder

Today's Data Center

We Have Control

It's located at X.
It's stored in server's Y, Z.
We have backups in place.
Our admins control access.
Our uptime is sufficient.
The auditors are happy.
Our security team is engaged.

Tomorrow's Public Cloud

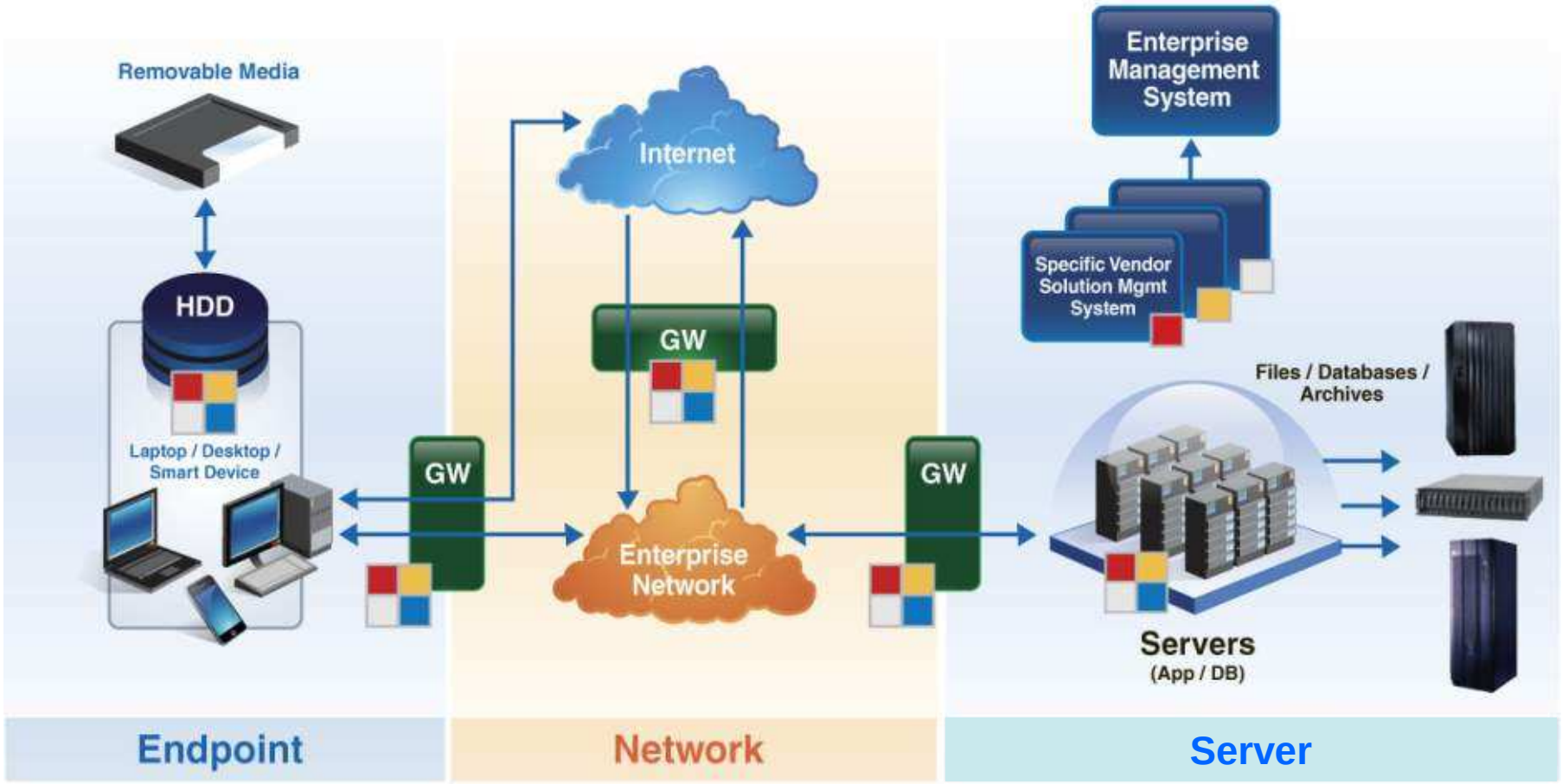


Who Has Control?

Where is it located?
Where is it stored?
Who backs it up?
Who has access?
How resilient is it?
How do auditors observe?
How does our security team engage?

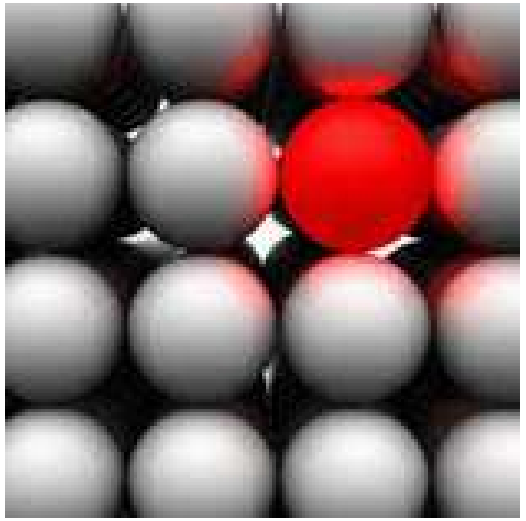
Data security requires a holistic framework across the key control points

Captured > Stored > Transmitted > Used > Archived > Modified



Protecting key business information at key control points

- From a business perspective, the level of security protection applied must be based on the business value of the information that is protected
- The business value of data must drive the IT security controls that are implemented
- This idea is at the heart of the IBM Data Centric Security Model

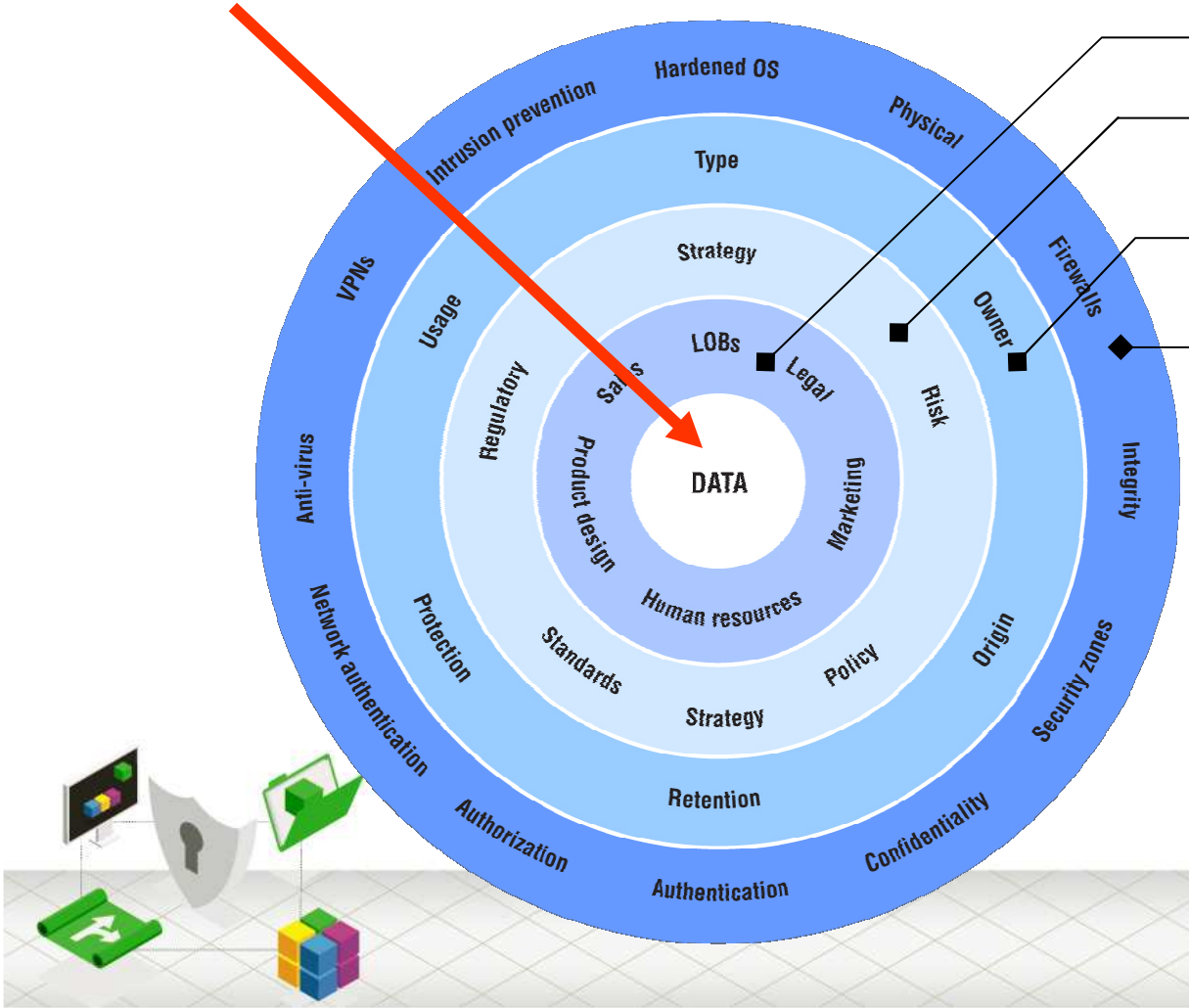


Our methodology leverages IBM's thought leadership in data-centric security

- Developed by IBM Global Business Service in 2006 - Patented method for analyzing data security
- Uses the **business value of data** to determine and implement the **appropriate level of overall IT security**
- The DCSM does not depend explicitly on specific security products or technologies and may be seen as independent of the underlying security infrastructure

The IBM Data Centric Security Model ….the starting point for an an effective Information Security Governance

Information Security starts at Data level …..
….. we must shift focus from the **T** in « IT Security » to the **I** …



Data owner and custodian

Corporate and regulatory guidelines

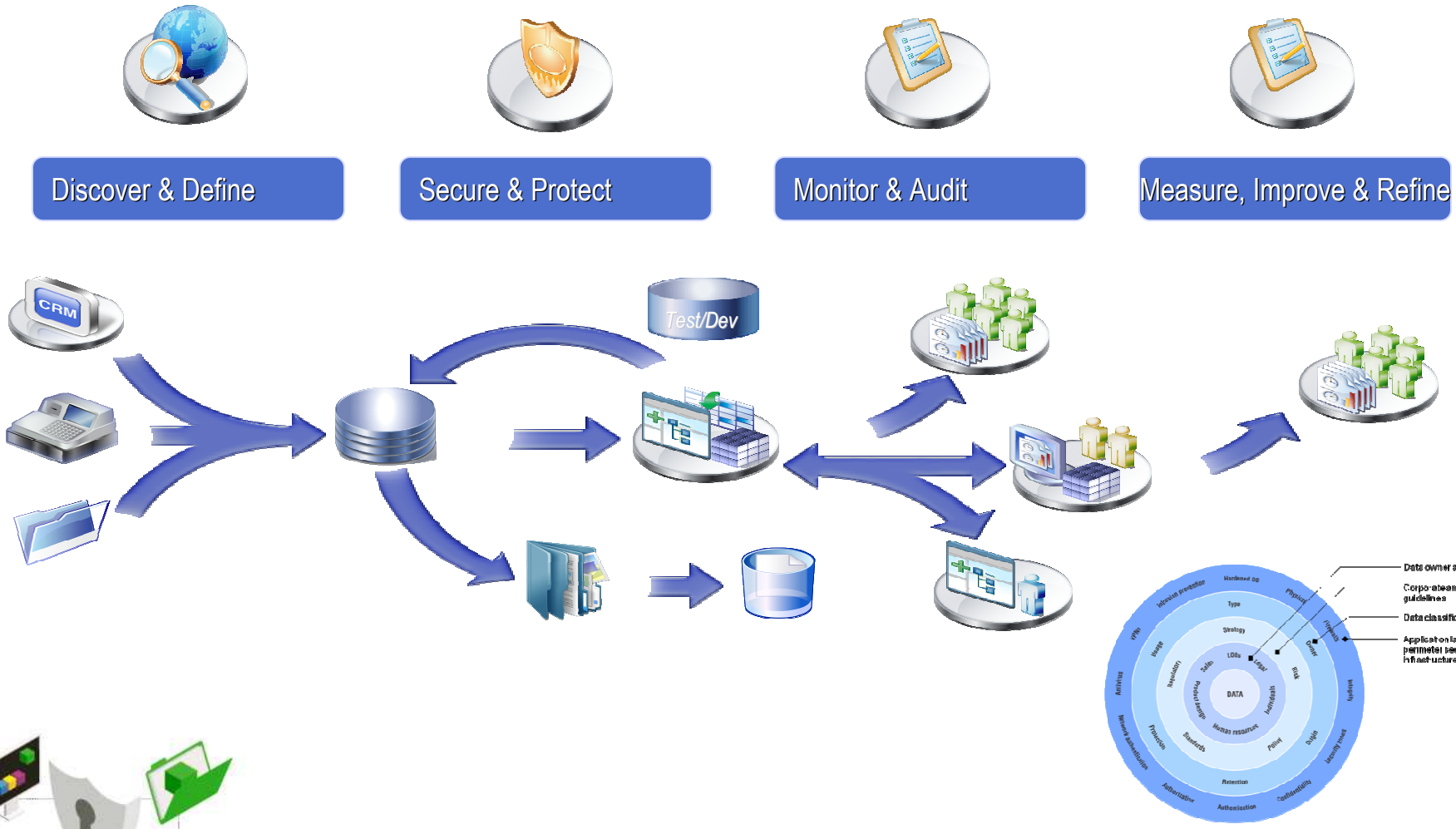
Data classification

Application layer and perimeter security infrastructure

We understand the problem and we have the solution

- Data Security is a **Business** problem
- **Technology** as a business enabler

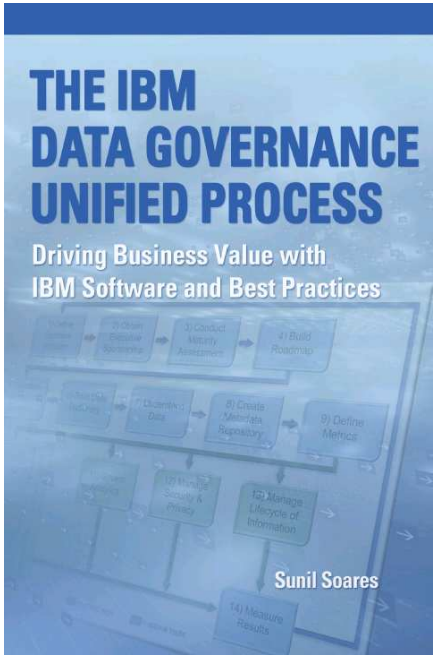
IBM Data Governance Unified Process for Security & Privacy



IBM Data Governance Unified Process for Security & Privacy

12. Security & Privacy:

- 12.1 Define sensitive data
- 12.2 Discover sensitive data
- 12.3 Classify and tag sensitive data
- 12.4 Protect sensitive data
- 12.5 Encrypt sensitive data
- 12.6 Monitor database activity by privileged users
- 12.7 Monitor applications for fraud
- 12.8 Prevent against Cyber attacks
- 12.9 Tighten database change controls
- 12.10 Measure, Improve and Refine

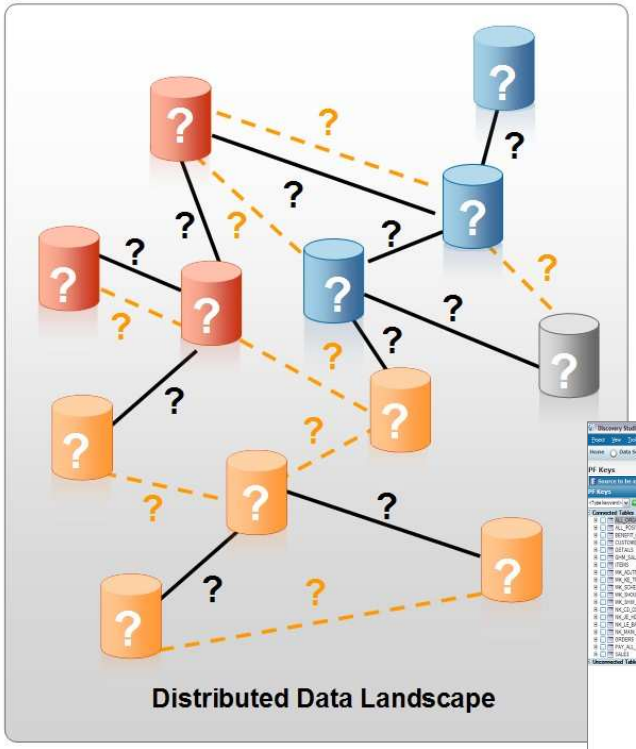


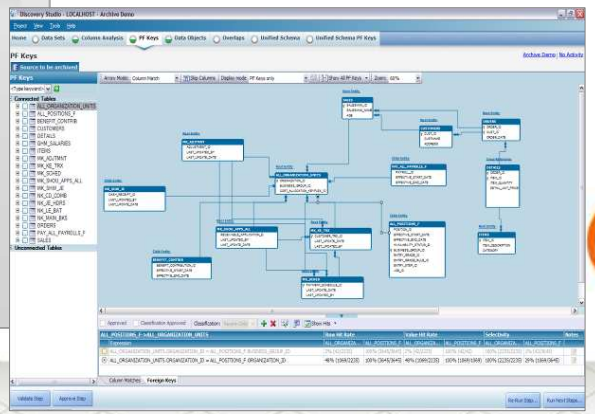
IBM

Discover & Define

Define, Discover and Classify Sensitive Data

- Where does the data live today ?
- Which data is sensitive ?
- How data is related and may be hidden ?
- Which data can be shared ?





Sensitive Relationship Discovery

System A Table 1

Number	Name
3544600986	Alex Fellthan
5728	
3786	
6783	Bob Smith
4035567193	Eileen Ranchman
8037409934	Fred Simpson
4306123913	George Brett
9525061085	Jamie Slattery
4594182715	Jim Johnson
1288966020	Martin Aston

Patient ID # embedded within another field

System A Table 15

Patient	Result	Test
3802468	N	53
		53
		32
	N	53
5567193	N	72
6123913	Y	47
6736304	N	34
7409934	N	34
8150928	N	47
8966020	N	34

System Z Table 25

Code	Name
53	Streptococcus pyogenes
72	Pregnancy
32	Alzheimer Disease
47	H1N1
34	Dermatamycoses

Encrypt Sensitive Data
In addition to confidentiality, encryption delivers …

Ensures broad threat defense against
- Lost or stolen media
- Unauthorized file sharing
- Privileged user abuse
- Data leakage / unauthorized access
- File protection: backups, log, configuration, executable

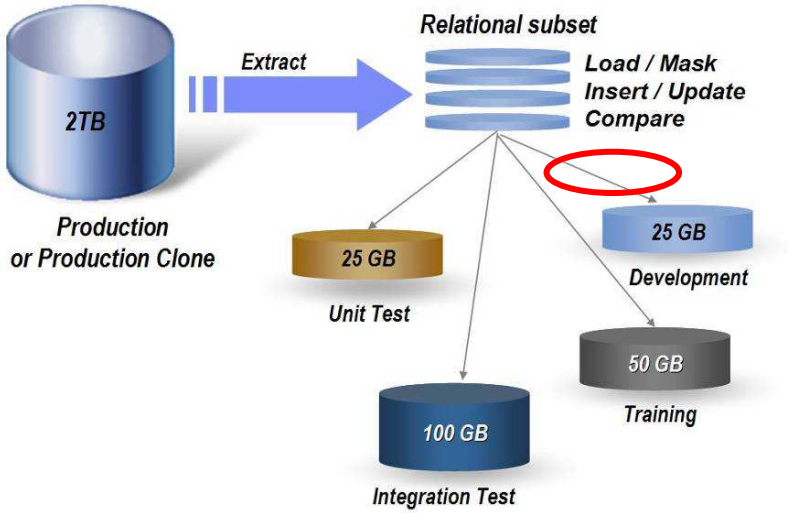
Helps satisfy compliance requirements
- Regulatory standards
- PCI-DSS, SOX, PII, HITECH, GLB, etc.
- Corporate / internal mandates

Promotes separation of duties
- Security management
- Technical staff
- Business owners

IBM
Secure & Protect

Secure and Protect Sensitive Data within non-Production environments

- Mask or de-identify sensitive data
- Data is realistic but fictional
- Support referential integrity of the masked data elements



Personal Info Table

PersNbr	FirstName	LastName
10000	Jeanne	Renoir
10001	Claude	Monet
10002	***Pablo***	***Picasso***

Referential integrity is maintained with key propagation

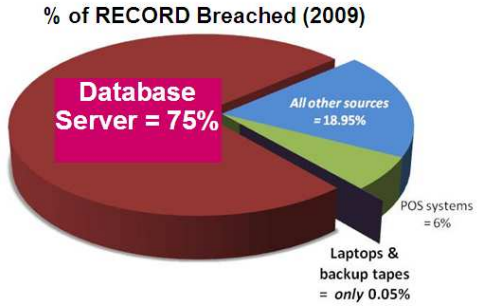
Event Table

PersNbr	FstNEvtOwn	LstNEvtOwn
10002	***Pablo***	***Picasso***
10002	***Pablo***	***Picasso***

IBM
Monitor & Audit

Monitoring Database Activity to detect and prevent Fraud

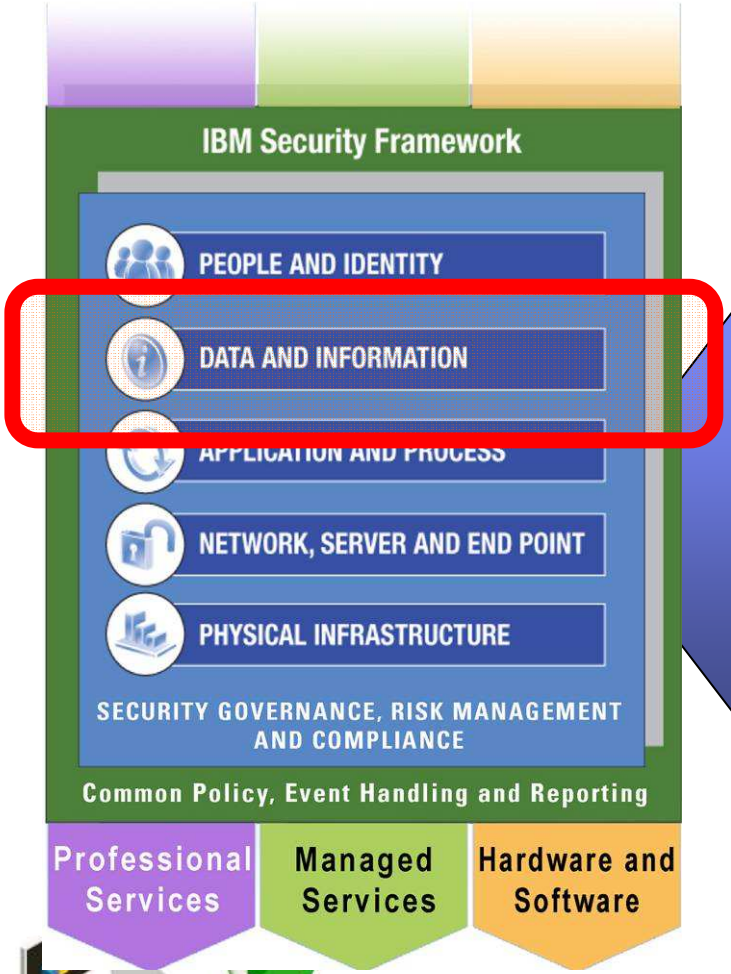
- Continuous, real-time database access and activity monitoring
- Detect unauthorized or suspicious activity
- Vulnerability assessment, change auditing and blocking
- Compliance reporting & escalations (SOX, PCI, NIST, etc.)



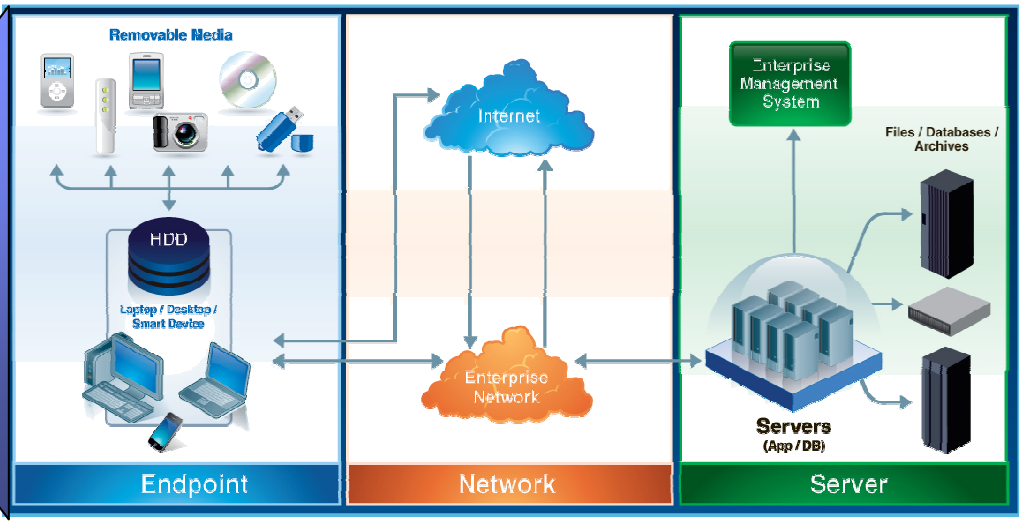
DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i=? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?,?)

Protecting Data is a key capability of IBM's Security Framework



Reduce cost and complexity of data protection by managing and optimizing across key control points

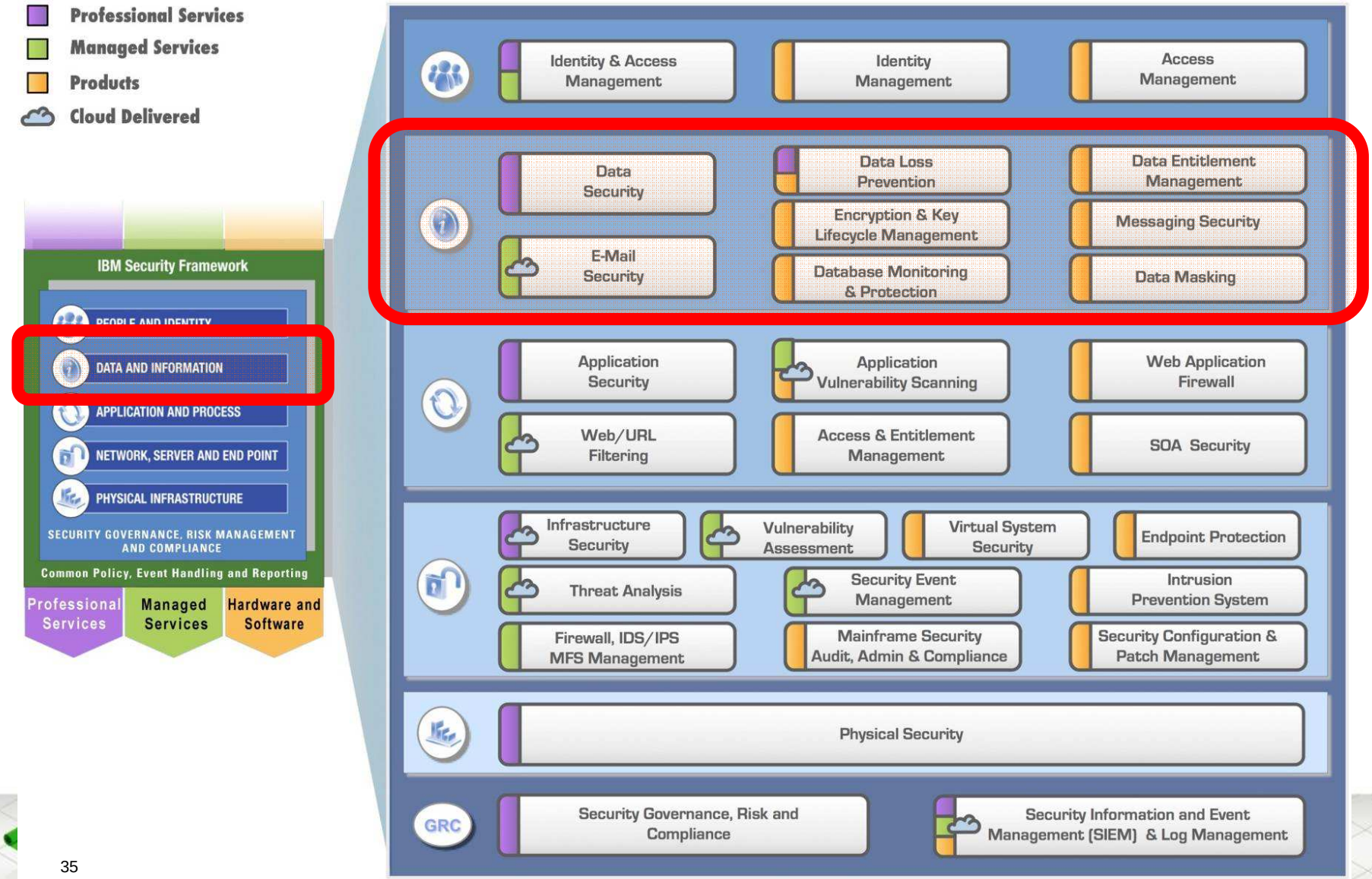


Focus on blocking data leakage

Focus on securing data in motion

Focus on securing the data center

Protecting Data is a key capability of IBM's Security Framework



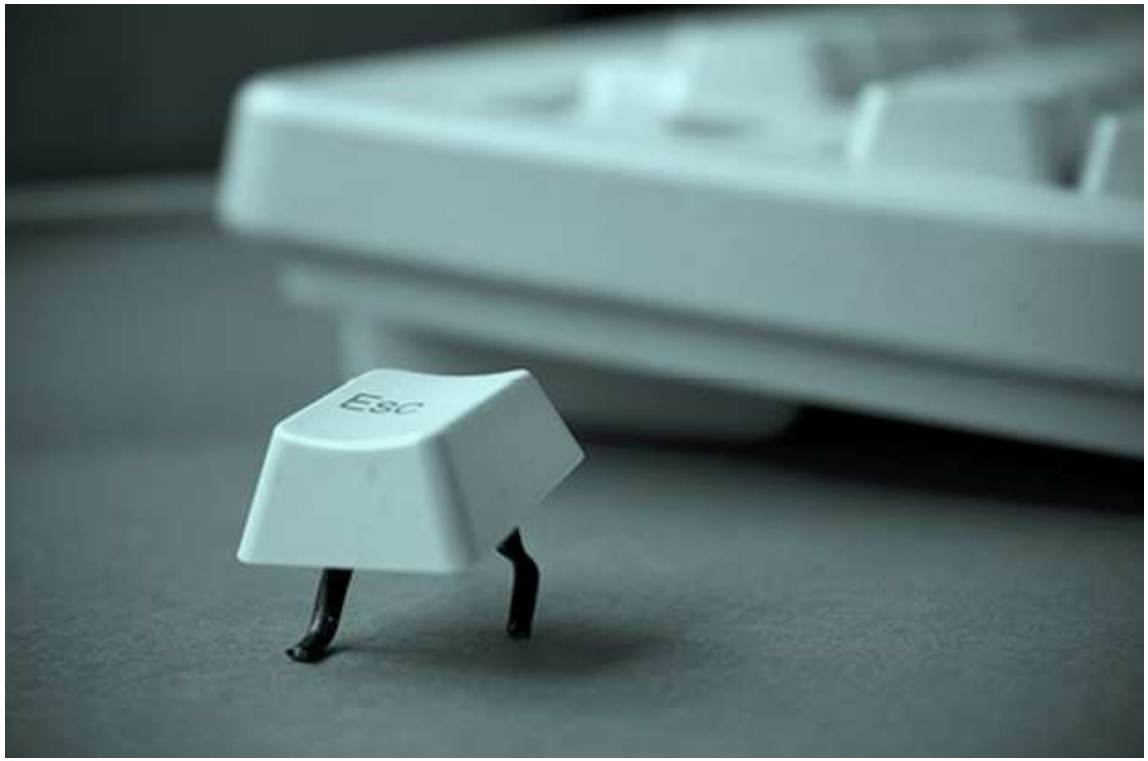
Are your critical data safe from today's evolving security threats ?

Sony data breach hits 77m PSN and Qriocity users
27 April 2011

The PlayStation Network has been taken down after a security breach, which has potentially compromised up to 77 million users' personal details. The name, address, date of birth and potentially the credit card details of up to 77 million users have been stolen in what is believed to be one of the biggest-ever online data breaches

.. If you have provided your credit card data through PlayStation Network or Qriocity, to be on the safe side we are advising that your credit card number (excluding security code) and expiration date may also have been obtained ….

Grazie



Tiziano Airoldi *tiziano.airoldi@it.ibm.com*
IBM Senior Certified Executive Architect