

Deloitte.

Security & Privacy webcast series

Session 1

A risk-based approach to data protection

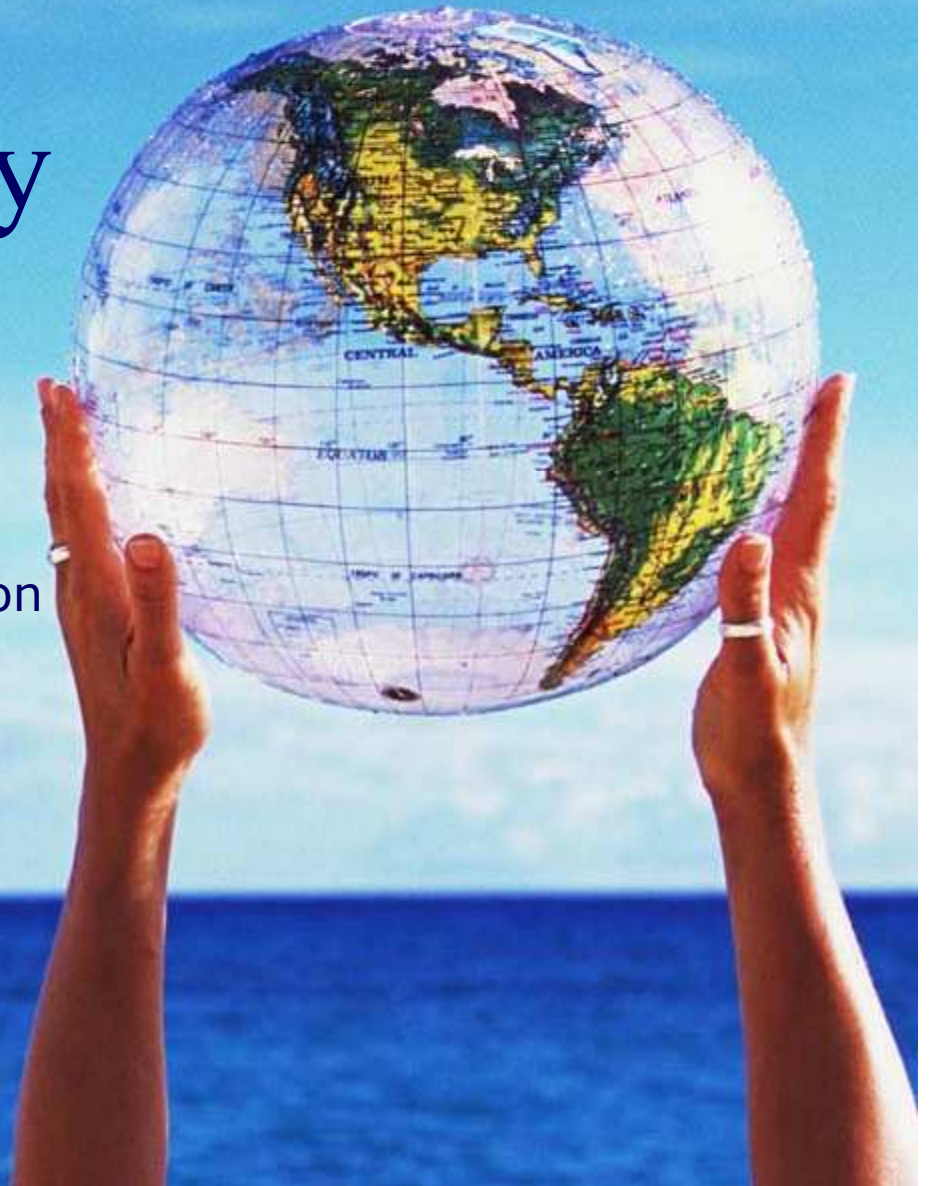
Reza Kopaei

rkopaei@deloitte.ca

416-997-2824

October 30, 2008

Audit . Tax . Consulting . Financial Advisory .

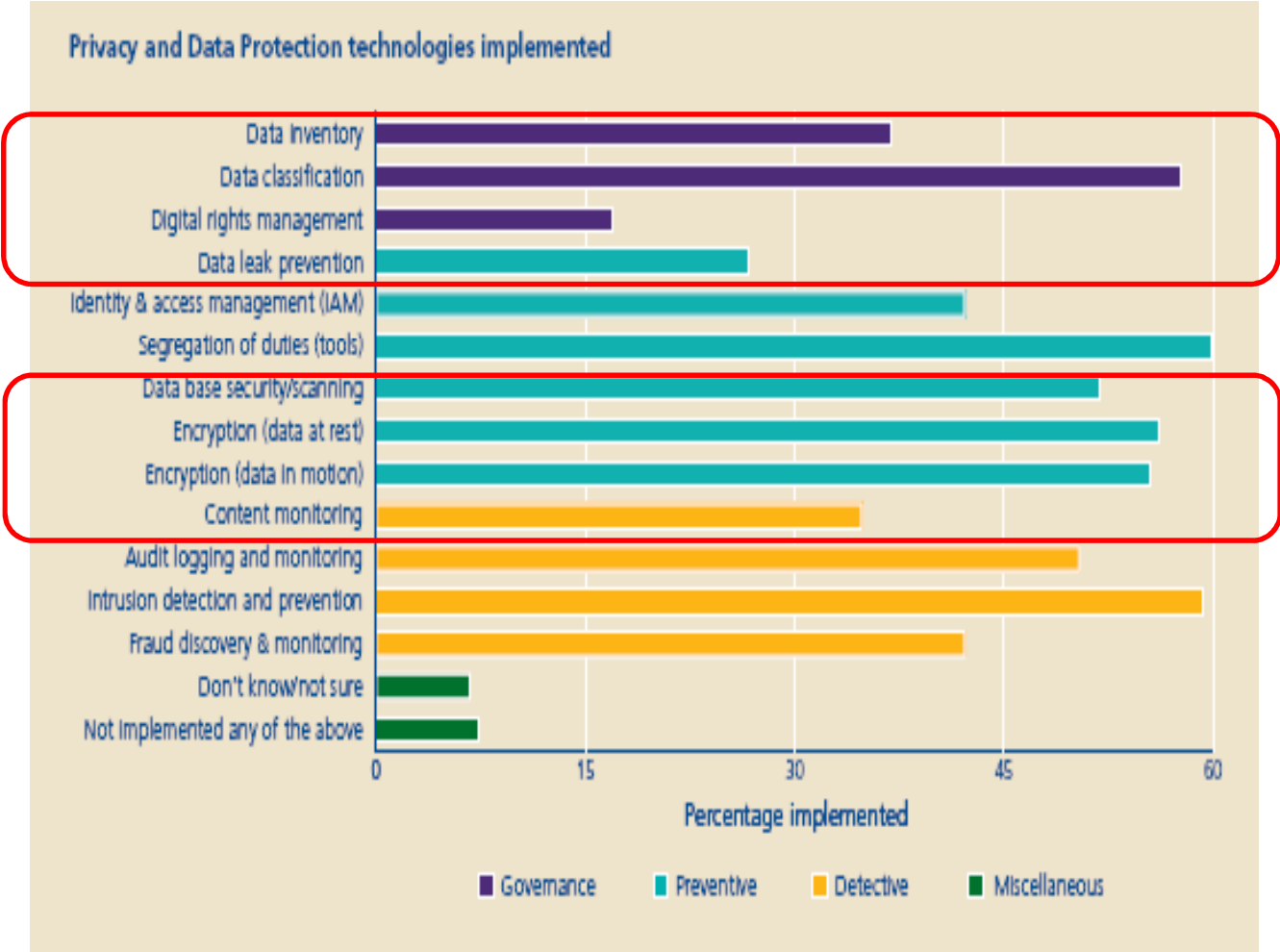


Webcast tips

- Make sure that your volume is turned up and your headphones are plugged in
- A copy of the presentation and supplementary material can be downloaded by clicking on the handouts icon in the top right hand corner of the screen
- Make sure that your pop-up blocker is disengaged
- To ask a question, click on the Q&A tab on the toolbar and click “ask”

Marketplace activity

The Deloitte 2007 Privacy and Data Protection Survey Solution responses show that organizations are adopting data protection solutions



What is data leakage?

The **movement** of a **data asset** from an **intended state** to an **unintended**, inappropriate or unauthorized state, representing a **risk** or a potentially negative impact to the organization

Breach type	Data type	Threat agents type
<p>Lost or Stolen</p> <ul style="list-style-type: none"> ▪ Backup Tape = Back up tapes ▪ Laptop = Public places (e.g. airport) ▪ Mobile Device = Blackberry, phone ▪ Mobile Storage = CD, Flash memory ▪ Printed Copy = misplaced prints (public place) <p>Accidental</p> <ul style="list-style-type: none"> ▪ Software, Email = Wrong Email address ▪ Printed/Faxed = SIN printed on mailing labels ▪ Mail = FIN send to wrong addresses <p>Disposal</p> <ul style="list-style-type: none"> ▪ Laptop/Desktop/Mobile Devices/ Backup Tapes/Drives ▪ Prints/Hardcopies <p>Hacked</p> <ul style="list-style-type: none"> ▪ Web Application/ Email/ FTP / Wireless Network <p>Malicious</p> <ul style="list-style-type: none"> ▪ Viruses / Worms/ Forged Actions/Keylogger <p>Negligence</p> <ul style="list-style-type: none"> ▪ Production Data In Development Test Environment 	<p>Personal</p> <ul style="list-style-type: none"> ▪ CCN = Credit Card Number ▪ SSN/SIN = Social Security Number ▪ NAA = Name And / Or Address ▪ PPN /PII = Private Personal Information ▪ EMA = Email Address ▪ ACC = Account Number ▪ FIN = Financial Information ▪ MED = Medical Information ▪ DOB = Date of Birth <p>Business / Government</p> <ul style="list-style-type: none"> ▪ HR = Human Resources Information ▪ LG = Legal ▪ IP = Intellectual Property ▪ IIN = Intelligence Information ▪ FIN = Financial Information ▪ SLI = Sales Information ▪ MKT = Marketing Information 	<p>Insider</p> <ul style="list-style-type: none"> ▪ Malicious / Disgruntled Employee ▪ Contractors ▪ Outsourcers ▪ Business Partner / Vendor <p>Outsider</p> <ul style="list-style-type: none"> ▪ Script Kiddies ▪ Spies ▪ Gangs ▪ Ideologists ▪ Cyber terrorists ▪ Industry Espionage <p>Fraudster</p> <ul style="list-style-type: none"> ▪ Fraud ▪ Scammers (e.g. Phisher) ▪ Social Engineer

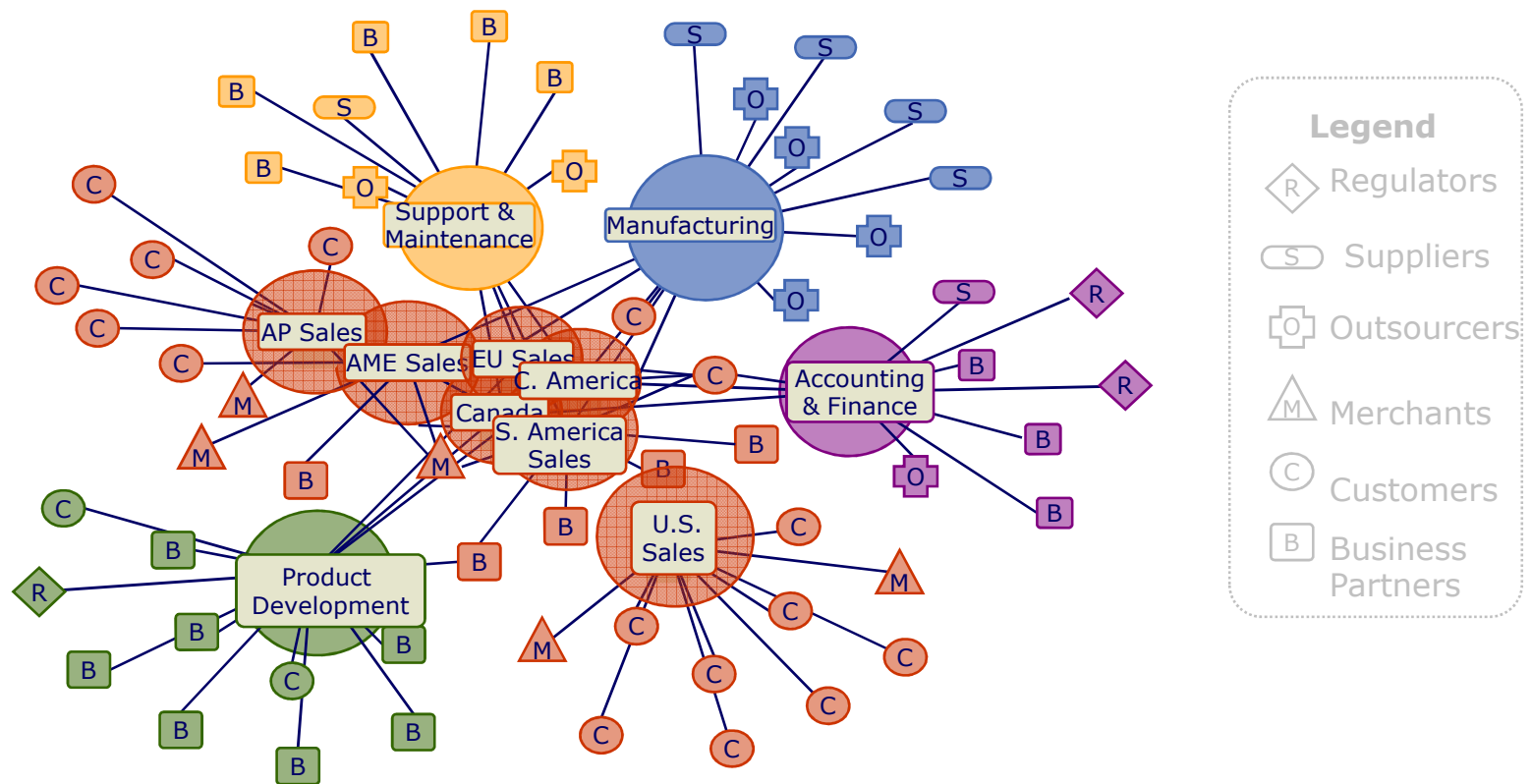
© Deloitte & Touche LLP and affiliated entities.

Data leakage problem

- Organization boundaries
- Organization processes
- Organization landscape
- Data growth
- Data asset
- Data valuation

Organizational boundaries

Organizational boundaries are changing as enterprises become more virtual, blurring the distinction between internal and external. At the same time, controls are required to manage the risk of unintended data transfer and usage



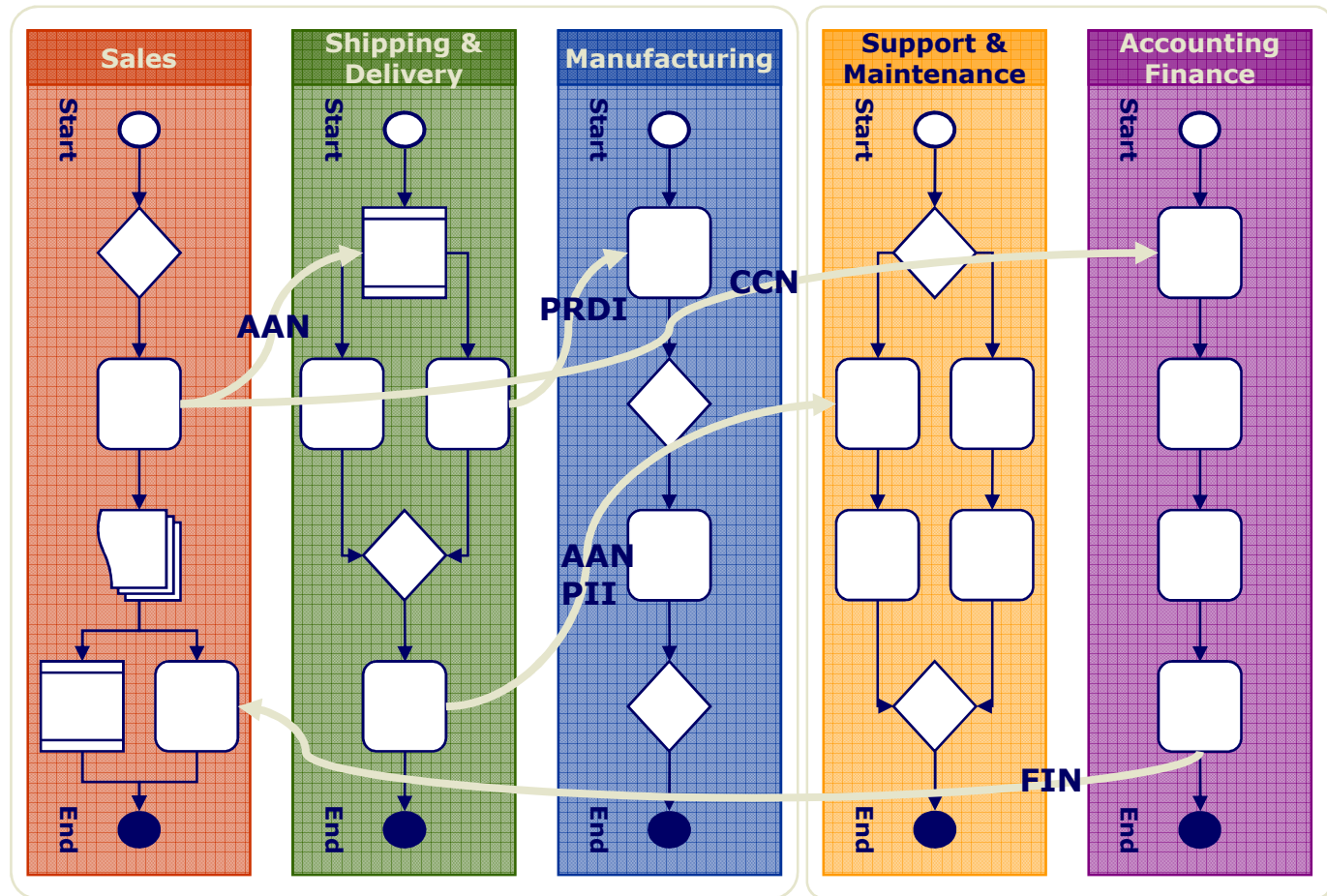
Perimeter centric security hinders business growth

Data flow and business processes

Sensitive data such as customer information, financial data, intellectual property moves horizontally across organizational boundaries, including vertical business processes (e.g., order fulfillment process). Organizations often do not have a good understanding of the movement, proliferation and evolution of their data

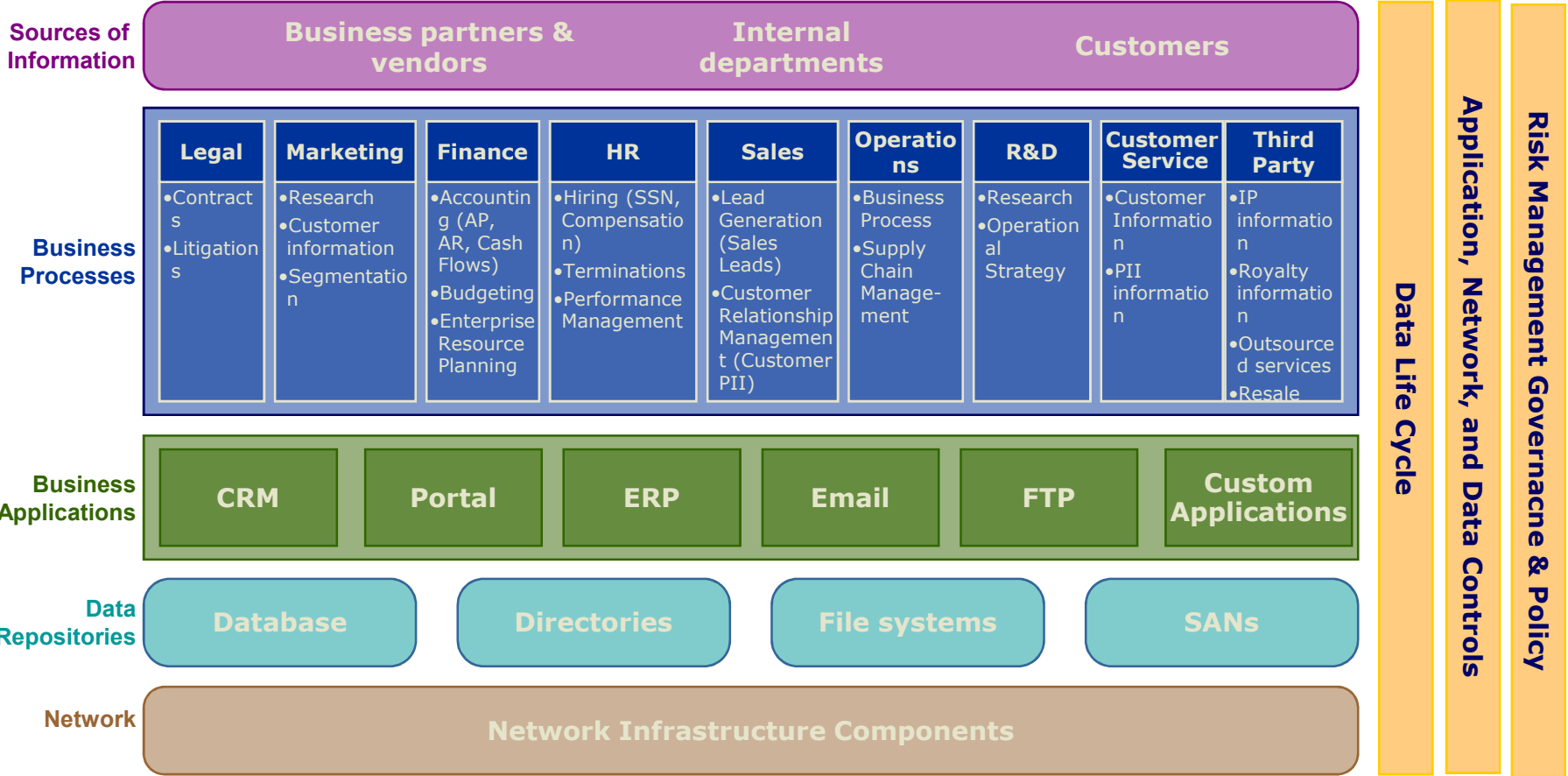
Segregation of duties results:

- No one has control over the entire process
- Few individuals know the entire process
- Organization does not know about the full data flow



Sensitive data in the organization landscape

Data from multiple sources is utilized by business processes and applications, and is stored in many data repositories

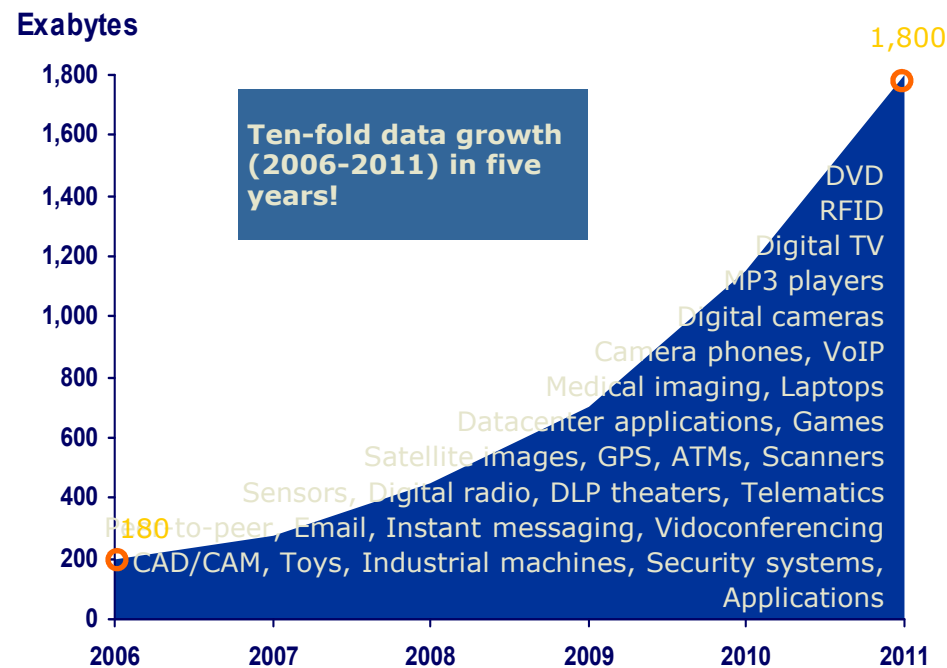


Today's organizations are: virtual, global, dynamic

© Deloitte & Touche LLP and affiliated entities.

Data growth

Declining cost of computing power, network bandwidth, and storage help to drive a rapidly expanding digital universe. IDC estimates worldwide annual data growth rates of 58% through 2011

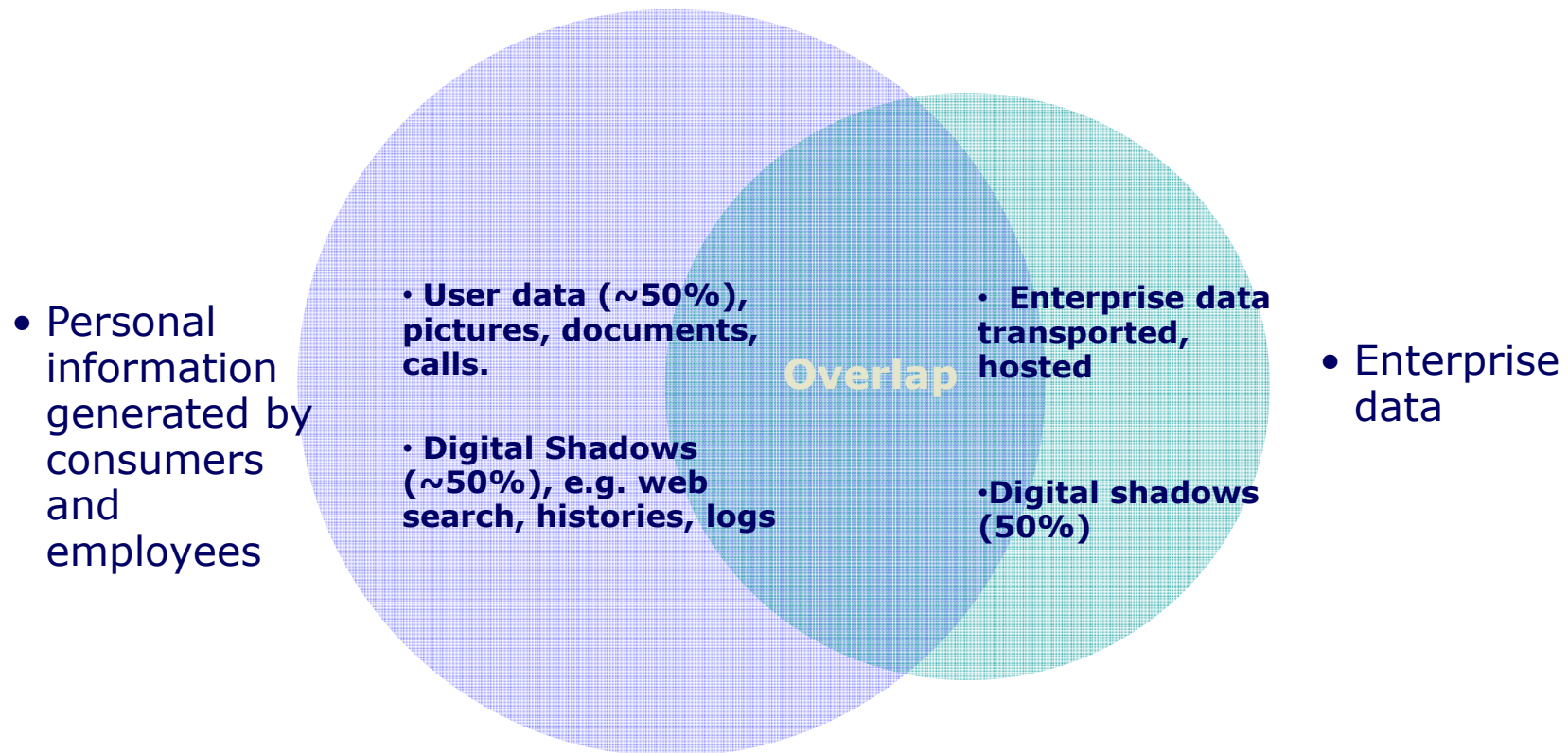


* Source: IDC Forecast of Worldwide Information Growth Through 2011

More data = more exposures

Expanding digital universe

Approximately 70% of the digital universe is created by individuals, but enterprises are responsible for the **security, privacy, reliability,** and **compliance** of 85%*

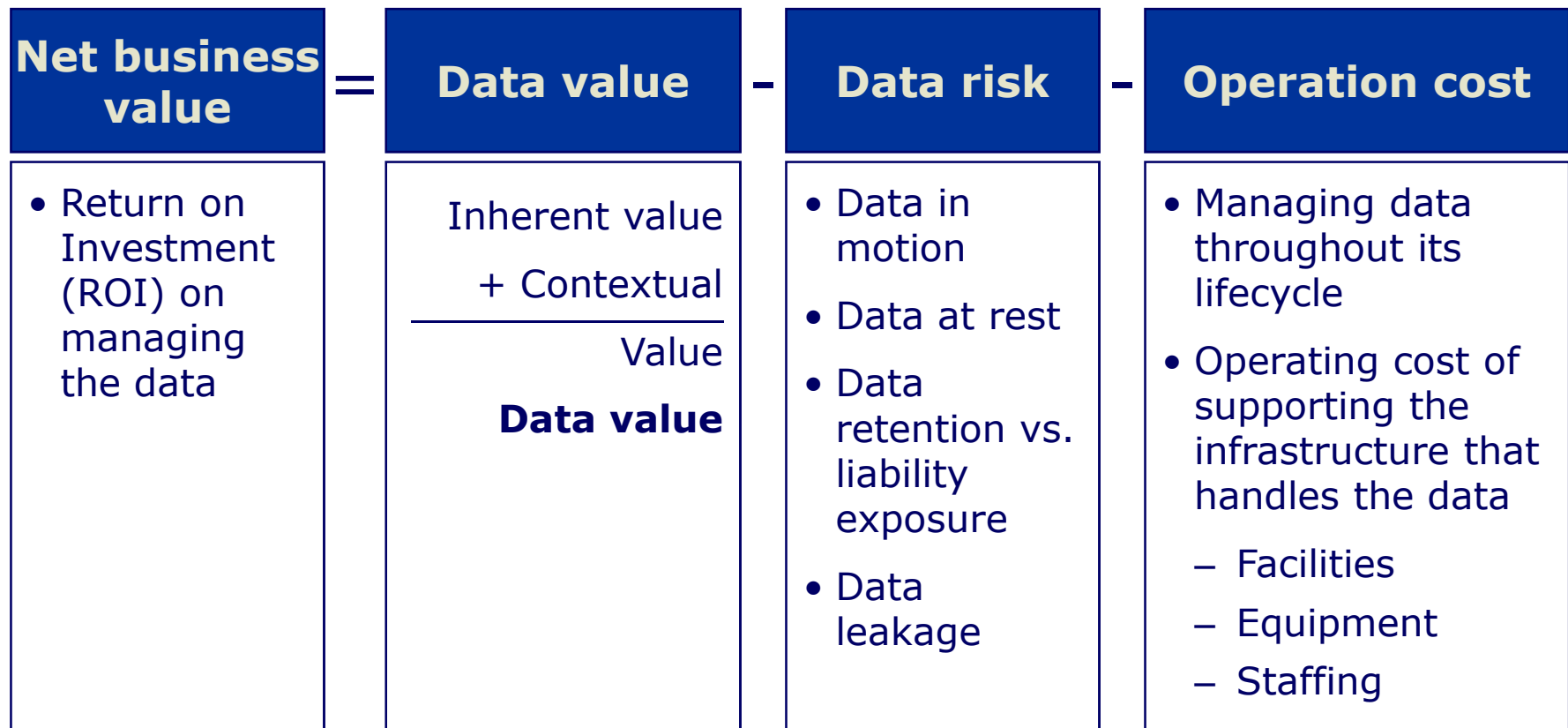


* Source: IDC Forecast of Worldwide Information Growth Through 2011

Information has half life

Analyzing data assets

Data can be managed like any other enterprise asset, subject to the same net business value calculations balancing value, risk, and total cost of ownership

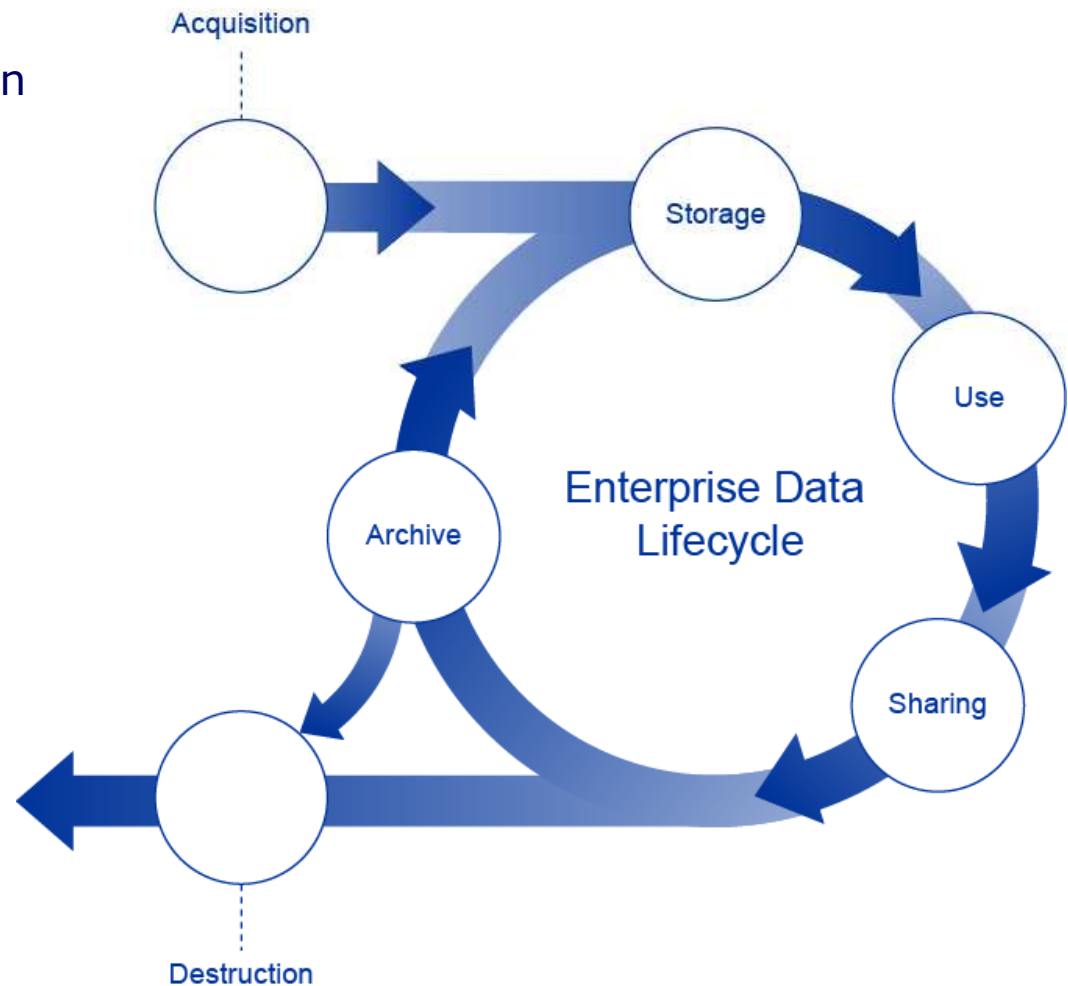


Data lifecycle – data leakage

The intrinsic and contextual value of data and associated ownership risk vary throughout the data lifecycle

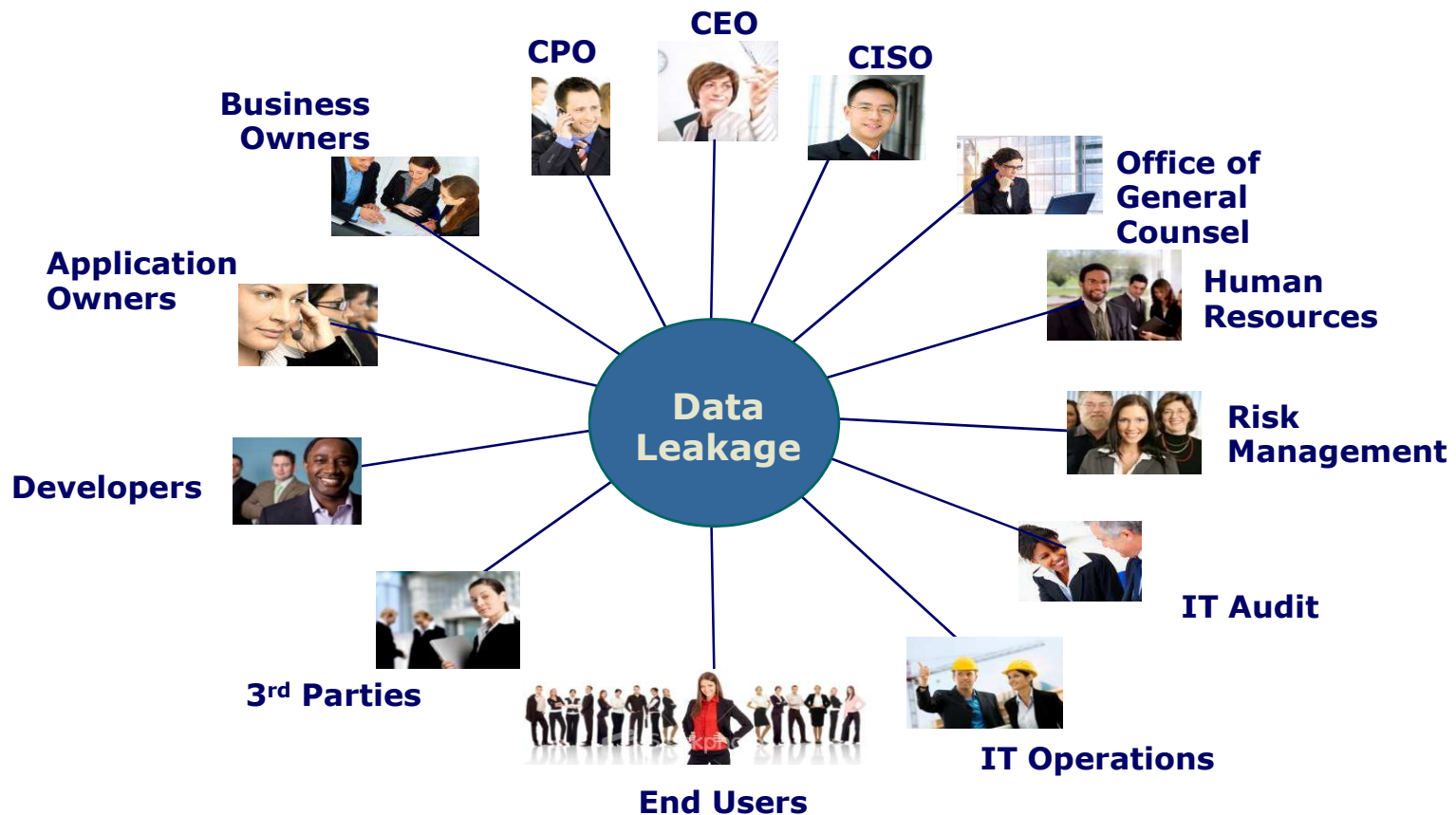
The business value of information assets – gains on process and function performance, revenue and margin contribution – are driven by:

- **Data attributes**
- **Enterprise context**
- **Associated risk**
- **Cost of ownership**



DLP stakeholders

DLP solutions provide services to multiple business applications, and involve a broad group of stakeholders. Understanding their concerns and perspectives is a key to DLP governance



Implications & drivers

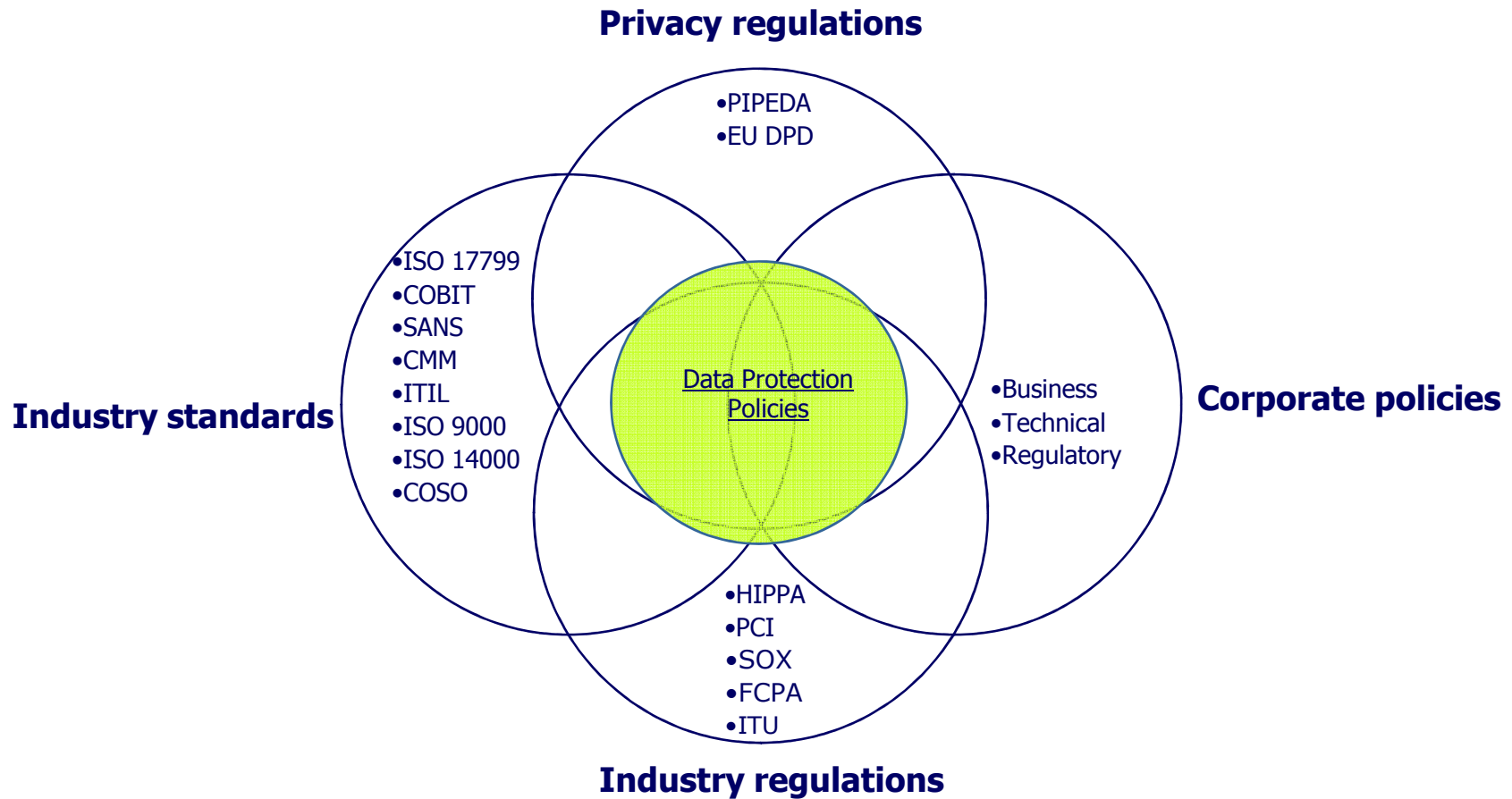
- Definition
- Organization boundaries
- Organization processes
- Organization landscape
- Data growth
- Data asset
- Data valuation

Data protection business challenges

Enterprises are realizing the business value of their data assets and are developing data protection strategies



Compliance



“Test once comply many times” reduces compliance risks and costs

Privacy laws



Cost avoidance & containment



Timely protection of data reduces cost of operation, incident handling, and legal discovery, and ongoing operational and maintenance costs

Category	Description
<i>Breach cost +</i>	Cost occurred per breached record
<i>Storage cost +</i>	Cost occurred per additional record maintained (hardware, software, storage cost)
<i>Litigation discovery cost +</i>	Cost of searching and preparing legal evidence and document
<i>Operation maintenance cost +</i>	Cost necessary to keep the lights on

Cost containment - data breach cost - three scenarios



Category	Description	1 Low-profile breach in a non- regulated industry	2 Low-profile breach in a regulated industry	3 High-profile breach in a highly regulated industry
<i>Discovery, notification, and response</i>	Outside legal counsel, mail notification, call center, and discounted product offers	\$50	\$50	\$50
<i>Lost employee productivity</i>	Employees diverted from other tasks	\$20	\$25	\$30
<i>Opportunity cost</i>	Customer churn and difficulty in getting new customers	\$20	\$50	\$100
<i>Regulatory fines</i>	FTC, PCI, SOX	\$0	\$25	\$60
<i>Restitution</i>	Civil courts may require funds be set aside to cover liability	\$0	\$0	\$30
<i>Additional security and audit requirements</i>	The security and audit requirements levied as a result of a breach	\$0	\$0	\$10
<i>Other liabilities</i>	Credit card	\$0	\$0	\$25
Total cost per record		\$90	\$155	\$305

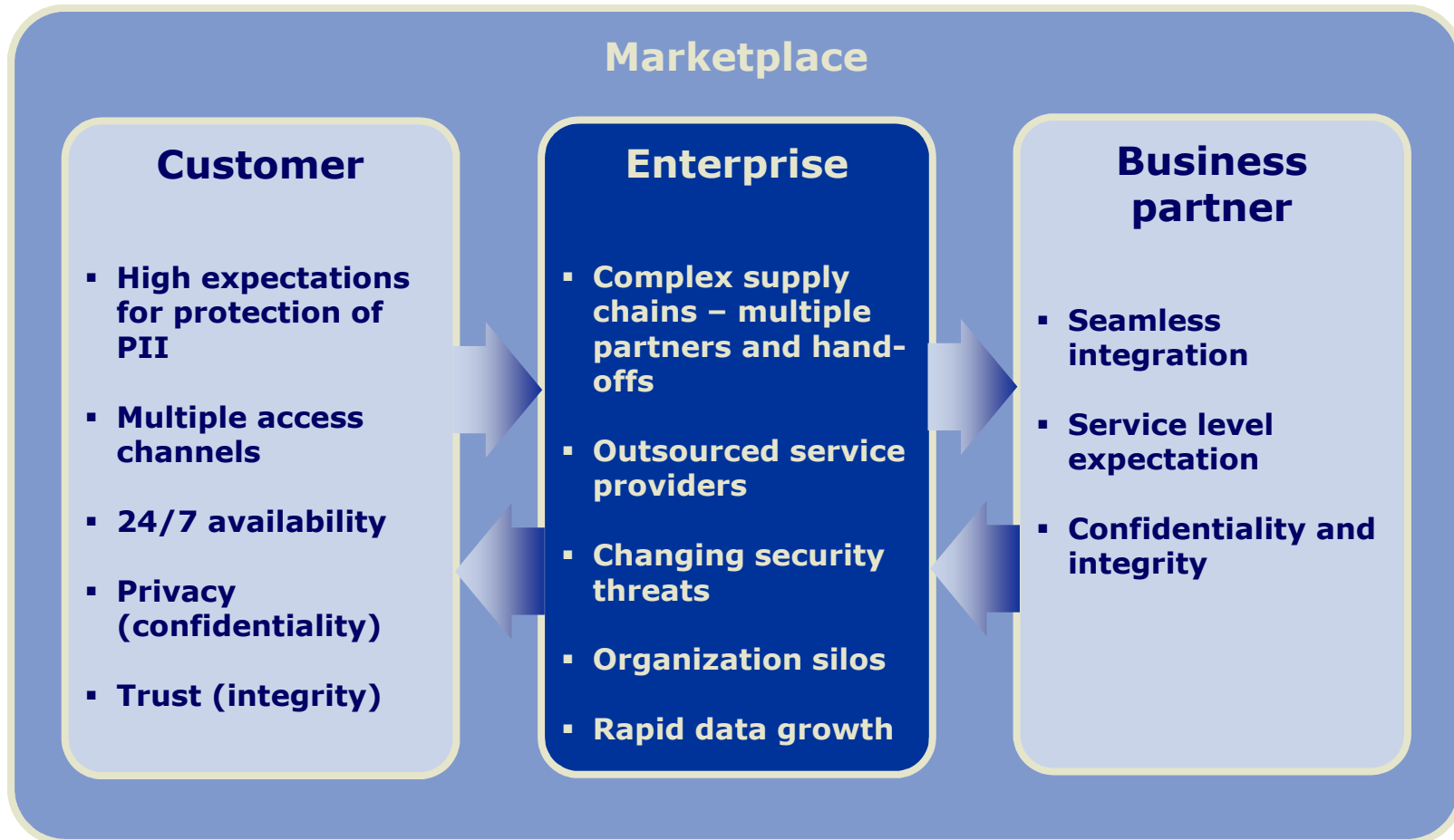
Source: Forrester Research: Calculating The Cost Of A Security Breach, April 2007

© Deloitte & Touche LLP and affiliated entities.

Business enablement



- Globalization
- 24/7 availability
- Merger & acquisitions
- Rapid technology changes
- New legal and regulatory requirements





Reputation & brand protection

Proactive steps for managing reputation and brand protection is necessary

Brand & reputation management

Crisis & incident management

Proactive brand monitoring

Prevent brand infringement

Overview

- ✓ In crisis people actions tend to be chaotic:
 - Build an incident/crisis management process and plan
 - Prepare a communication template/plan

- ✓ Proactively monitor media (online and printed form):
 - Monitor social media networking sites (e.g. YouTube, Wikipedia, email phishing)
 - Monitor newspaper, articles, word of mouth

- ✓ Proactively prevent brand infringements:
 - Contact ISP
 - Send cease and desist letter







“It takes 20 years to build a reputation and five minutes to ruin it. If you think about that, you might do things differently.” <<Warrent Buffett>>



Operational efficiency

Data proliferation across the organization and beyond results in operational inefficiencies

These inefficiencies apply to:

-  **Storage (tiered storage)**
-  **Archiving and backup**
-  **Knowledge and record management**
-  **Business continuity**
-  **Development & testing time**
-  **Compliance monitoring & reporting**

Without an effective method to:

- **Discover** data, it is difficult to apply the appropriate security controls to it;
- **Classify** data, it is difficult to understand the importance and sensitivity of the data;
- **Control** data, it is difficult to restrict access to data, prevent misuse of it, and secure it at rest and in transit;
- **Audit** data and its usage, it is difficult to enforce the security controls.

As a result, it is difficult to adequately **protect** data efficiently and effectively across the enterprise

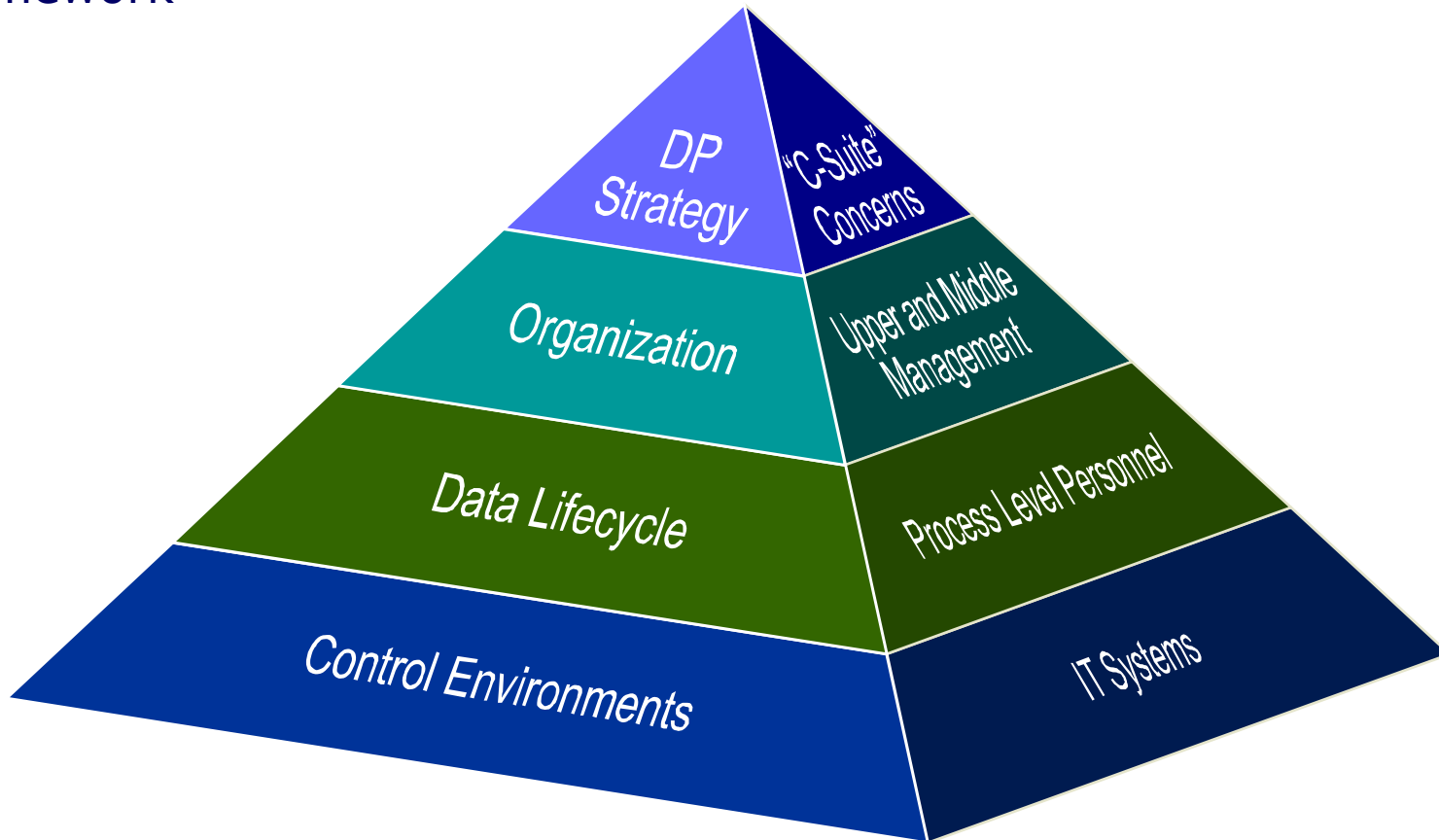
Most organizations have not adequately protected their sensitive data because of the magnitude and diversity of the problem...a single enterprise "silver bullet" does not exist

Data protection framework

- Framework
- Strategy view
- Organization view
- Data lifecycle view
- Control environment view

Data protection: a framework

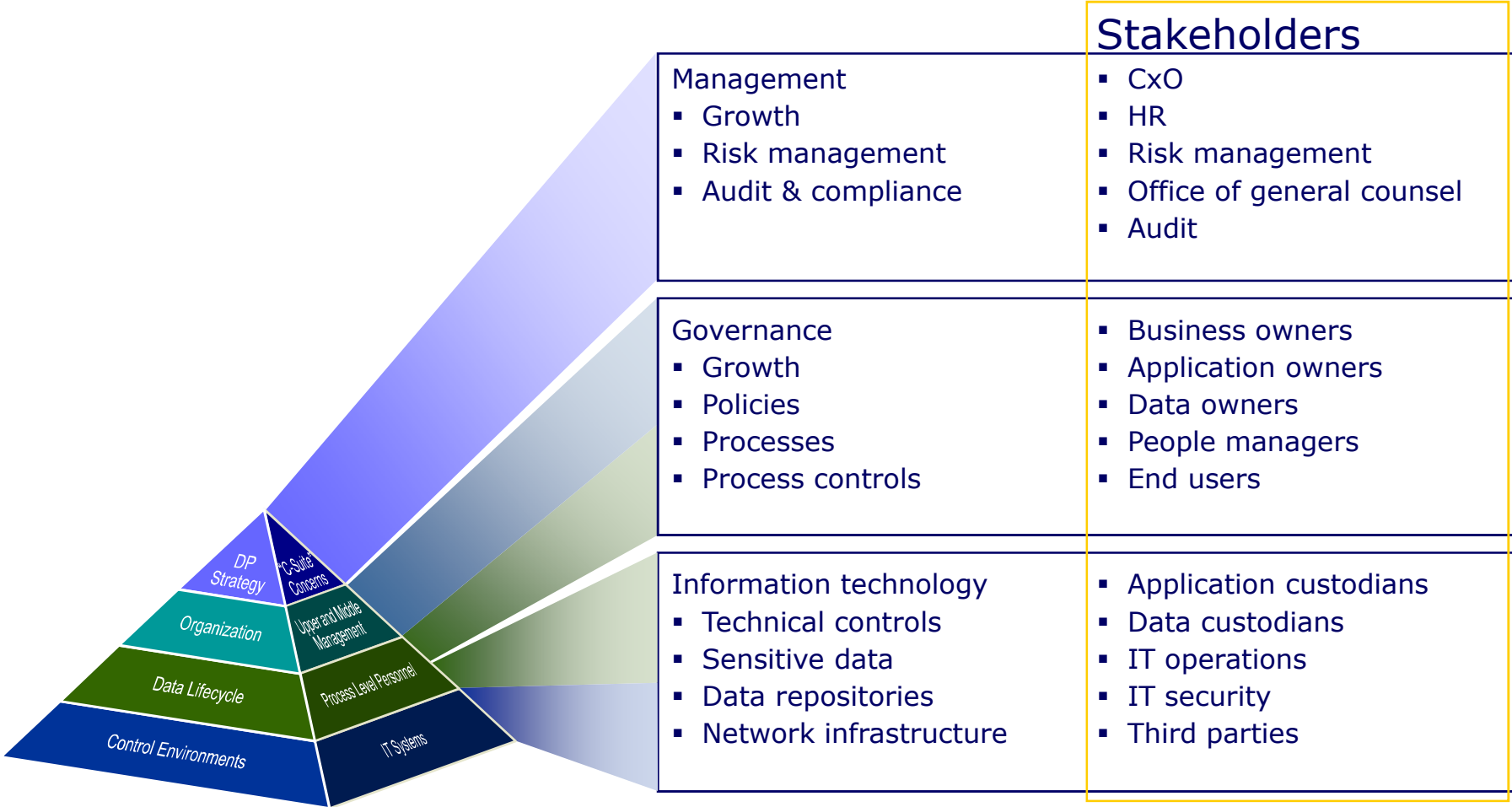
Addressing data leakage risks, providing appropriate protections requires a framework

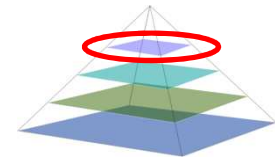


Security as a combination of people, processes and technologies is nowhere more evident than in the control of information across enterprise perimeters

Data leakage protection views

Data protection solutions can be described via separate but interrelated views tailored to specific stakeholder and project concerns.





Data protection strategy view

Develop a strategy for moving away from reliance on perimeter security, towards a risk-based and data-centric view

Current state:

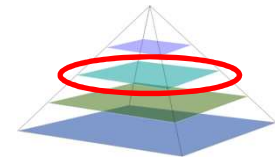
- **Rely on building walls around networks, servers, applications**



Goal state:

- **Apply security to the information assets themselves**

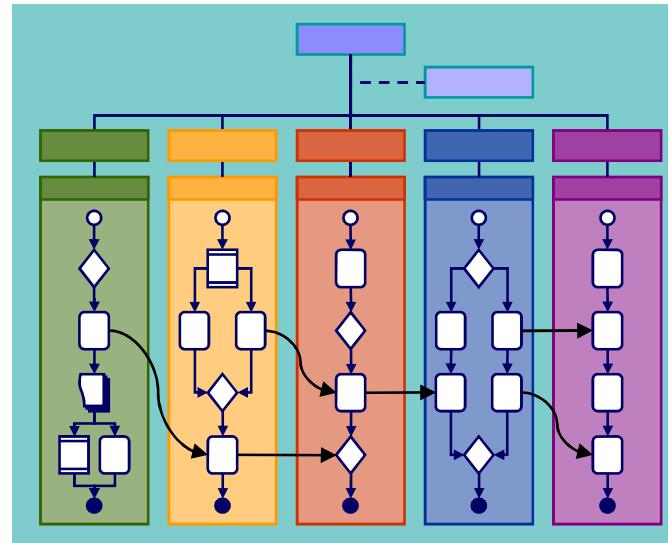
An end-to-end strategy considers ...a comprehensive overview of information assets and future business initiatives, compliance, privacy, points of entry, storage, channels, encryption, BCP/DR, DRM, backup, archive, disposition,...



Organization view

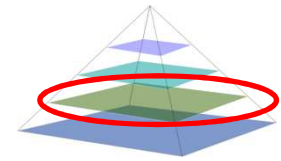
Focus on how the business uses data, identifies data flows across boundaries (geographic, organizational, process, system), inventories sensitive data and assesses data leakage risks

- **Define sensitive data**
- **Focus on high-risk business functions and processes**



- **Map sensitive data flows, based on how the business functions operate**
- **Identify business data owners**

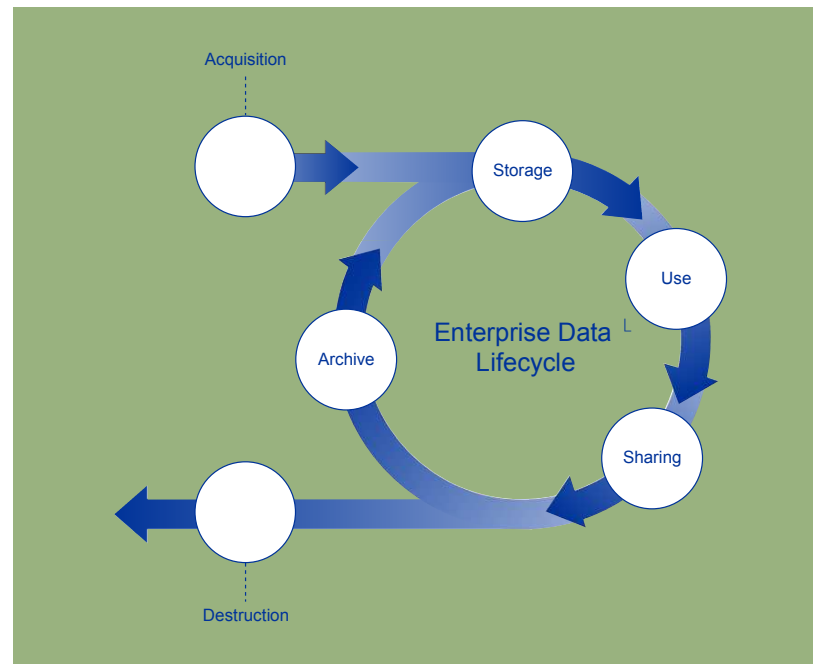
Given the data growth problem (70% annually) it does not make sense to apply a blanket information protection strategy. A functional view provides the next level of refinement



Data lifecycle view

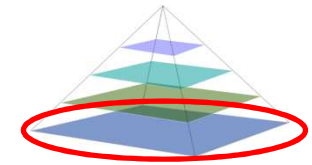
Develop a model for how sensitive data is acquired, created, stored, used, shared, archived and disposed. Relate the data lifecycle to supported business processes and the underlying infrastructure environments

- **Review existing data protection policies and procedures**
- **Determine external Needs**

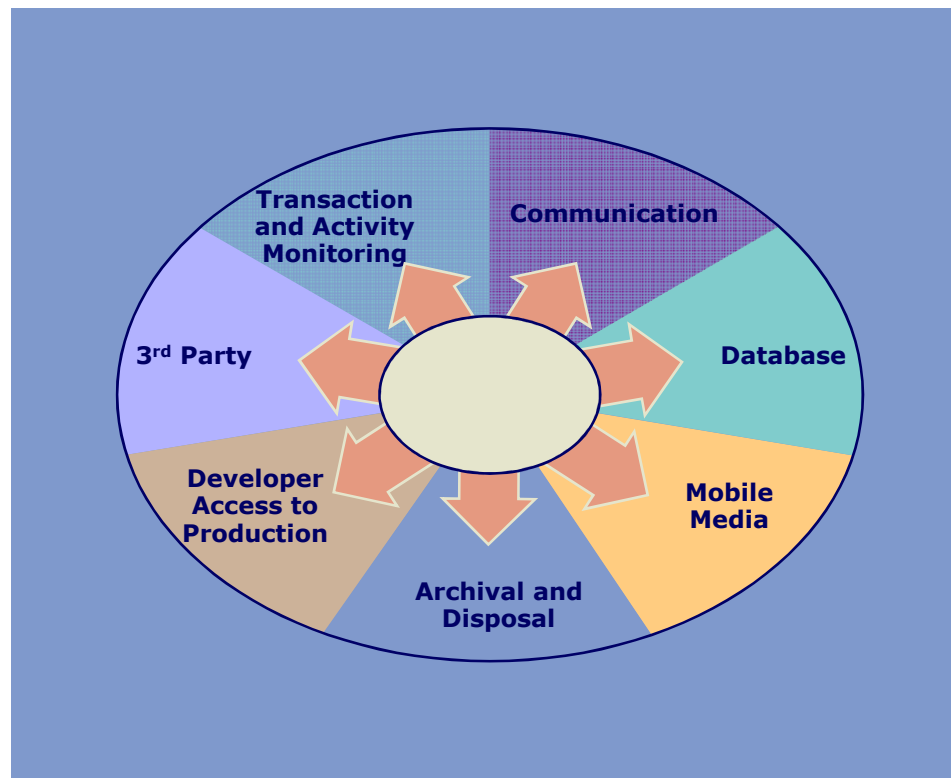


- **Model sensitive data lifecycle and how it flows through the business and where is captured, stored, used, and transferred**

Control environments view



Extend the risk-rationalized approach to map data flows through the relevant control environments and develop leakage controls

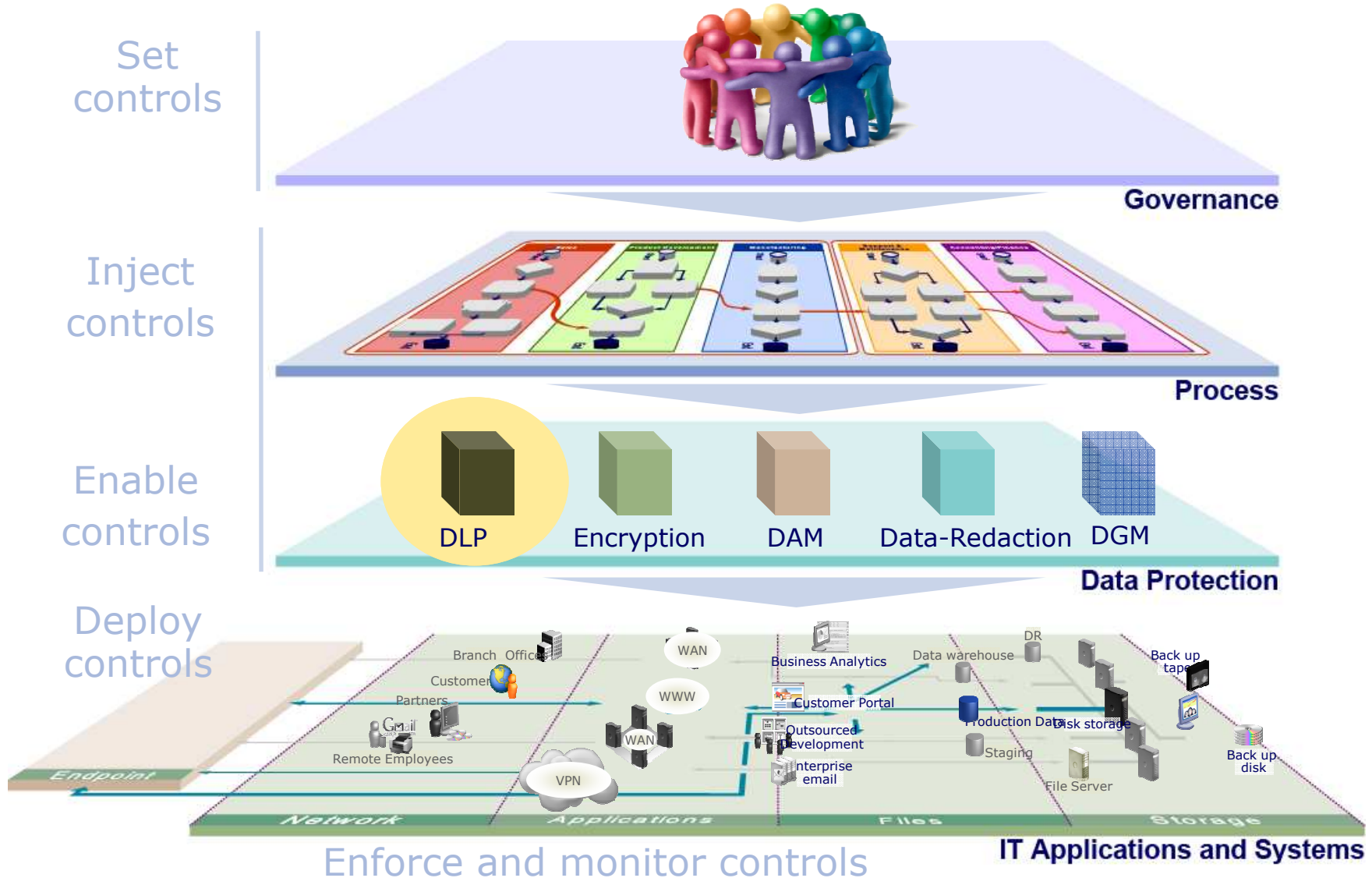


Implement environment-specific controls in order to reduce the **likelihood** and **impact** of data transfer from an **intended** to **unintended** state

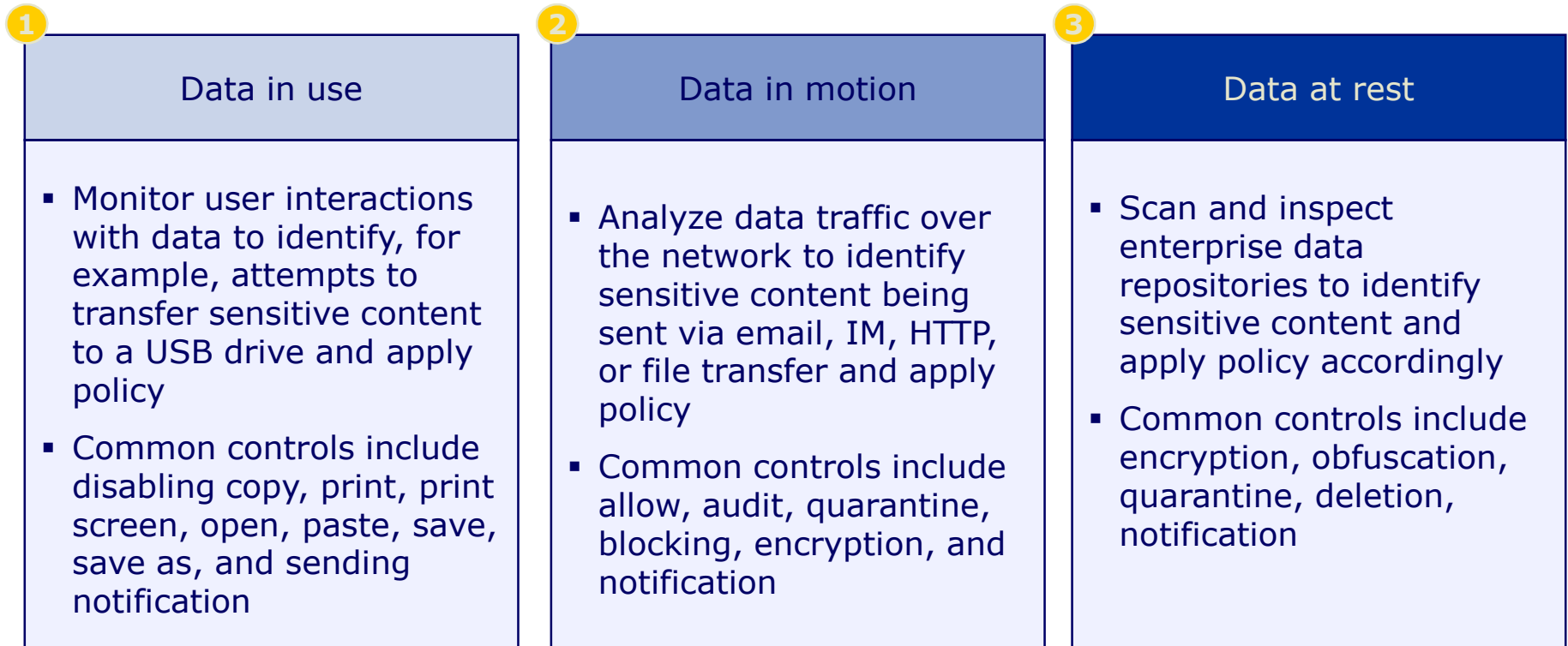
Data protection solutions

- DLP solution
- Strategy view
- Organization view
- Data lifecycle view
- Control environment view

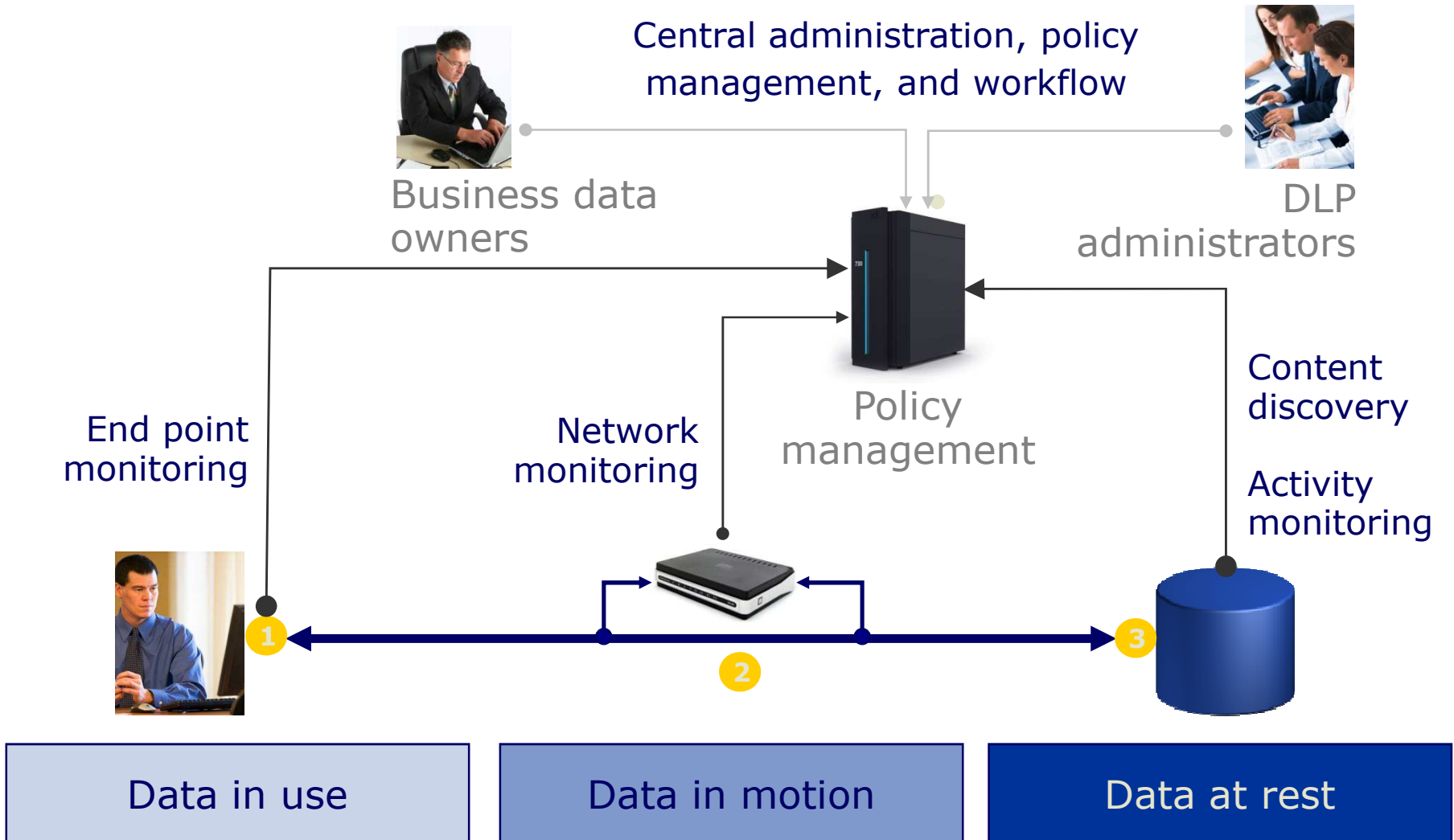
Data protection solution - conceptual architecture



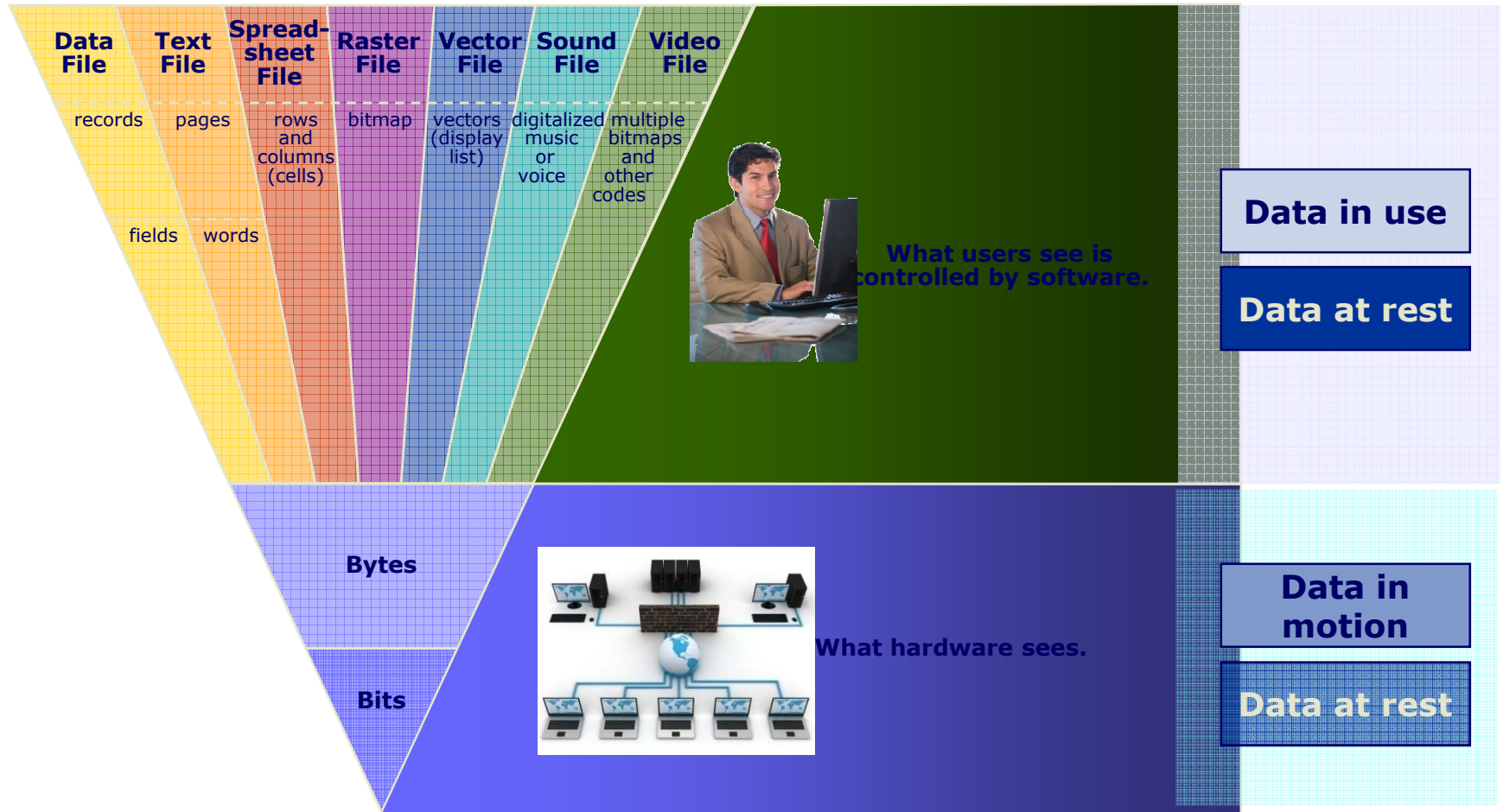
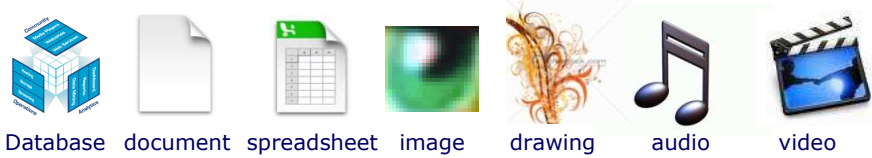
DLP solution functionality – simplified ILM



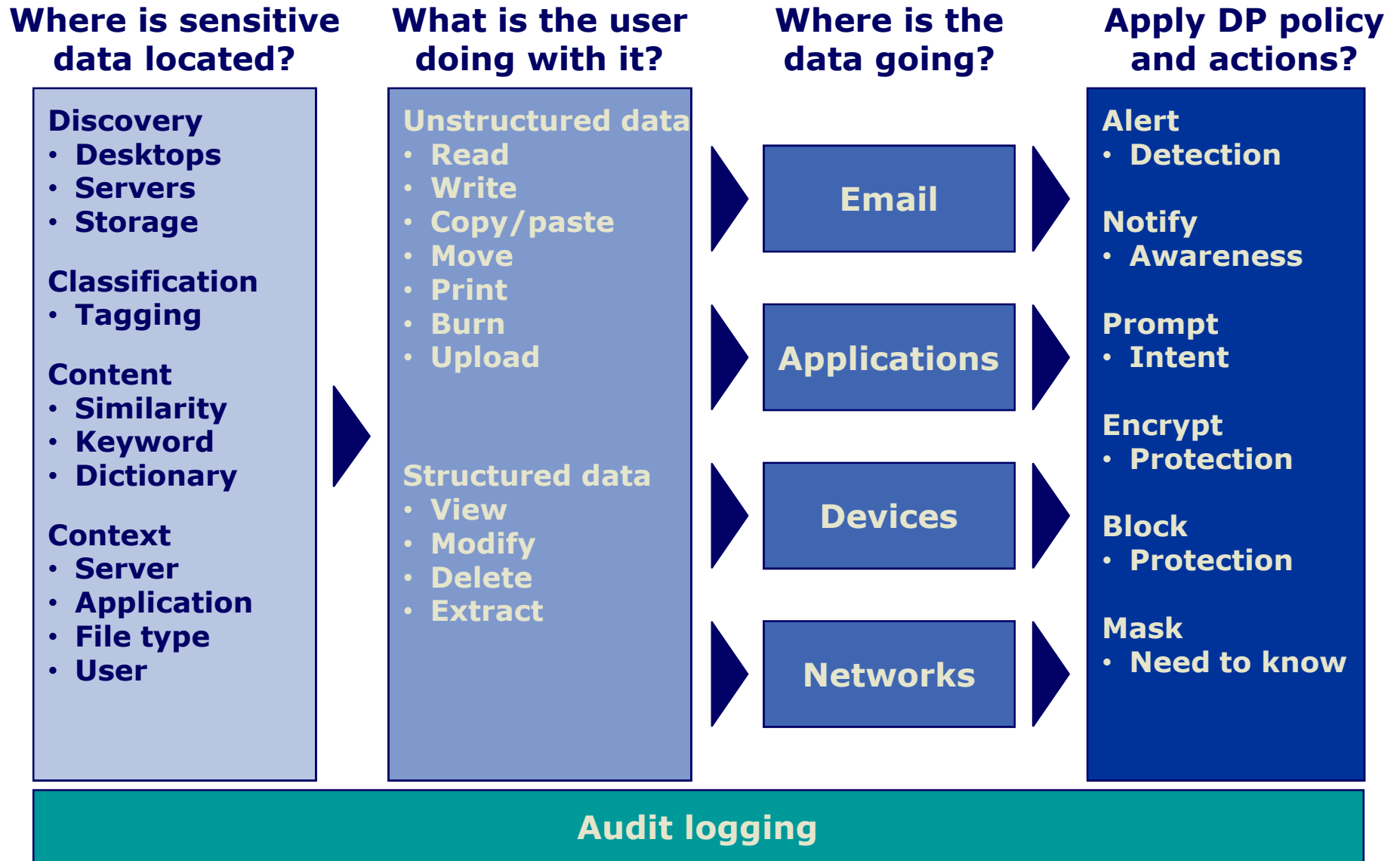
DLP solution conceptual model



DLP – deep content analysis



DLP – functional analysis



© Deloitte & Touche LLP and affiliated entities.

Source: Derived from "Data-Centric Security" IBM white paper (December 2006)

Data protection vendor products

<i>DLP</i>	<i>Encryption</i>	<i>DAM</i>	<i>Data redaction</i>	<i>Archive</i>	
RSA: Data Loss Prevention (DLP) Suite	RSA: Encryption and Key Management Suite	Guardium: Guardium	Ab Initio: Ab Initio	Symantec: Enterprise Vault File System Archiving	E-Mail and Filesystem
McAfee: Reconnex 7	Venafi: Encryption Key Management	Imperva: SecureSphere	Compuware: File-AID	Zantaz: Enterprise Archive Solution for Files	
Symantec: Vontu 8	Application Security: DbEncrypt	TIZOR: Mantra	DCR: DataVantage Global	Open Text: Livelink File System Arch	
Vericept: Monitor, Protect, Discover, Edge	Cisco: IronPort	Application Security : DbProtect	IBM: Optim	Applimation: Informia Archive	Database
Websense: Content Protection Suite	McAfee: SafeBoot Content Encryption, Device Encryption	Lumigent: Audit DB	Verdasys: Digital Guardian	IBM: Optim	
	Oracle, IBM, Microsoft: Native database encryption			OuterBay Technologies: LiveArchive	

Case study

- DLP solution
- Data redaction strategy
- Encryption strategy

Data protection technologies – communications environment

Major Canadian bank	
Large Canadian financial services firm	
Business problem / engagement type	Engagement duration
<ul style="list-style-type: none"> Increasing use of corporate email, webmail, instant messaging, and peer-to-peer and other channels for distributing data makes control of sensitive information leaving an organization a complex challenge Employees send emails that frequently contain confidential information to other employees and customers, who in turn may send it to a third party 	<ul style="list-style-type: none"> 8 weeks
Approach summary	
<ul style="list-style-type: none"> DP Strategy & Roadmap for communication environment outlining need for governance improvement, process re-engineering, new DLP and encryption technologies, integrated with the existing email and web applications Deployed DLP to monitor structured and unstructured data as it passes through the Communications Environment connecting the bank to its customers, business partners, and employees 	<ul style="list-style-type: none"> Implemented email encryption to protect sensitive data sent between the bank and its primary partners. The bank's connection to its business partners were tightened using transport layer security Identified the need for proactive incident response for data security breaches, raising the bar for protection of sensitive customer data collected, stored, and used by client
Key success factors	Lessons learned
<ul style="list-style-type: none"> Support from upper management, business owners 	<ul style="list-style-type: none"> DP technology implementation requires business involvement, process changes, and user awareness

Data protection technologies – data growth management

Major Canadian retailer	
Large Canadian retailer	
Business problem / engagement type	Engagement duration
<ul style="list-style-type: none"> Increasing reliance on email for handling business transactions Email and PST files morphed into an storage for important business documentation Employees had emails that were more than 6 years old and mixed with business, transient, and personal emails Compliance with business record retention periods and ediscovery complications and cost 	<ul style="list-style-type: none"> 8 weeks
Approach summary	
<ul style="list-style-type: none"> Creating a strategy and roadmap consisting of policy, training & awareness, technology A clear policy for storage of business record and use of email for business and personal communication Providing a technology tool integrated with exchange to identify and flag aged emails. The solution directed the user to either flag an email as business record or personal or transient record 	<ul style="list-style-type: none"> Business record were stored in the permanent storage environment with adequate backup and archiving solution Personal records and aged transient business records are deleted after 6 months and after a month of grace period Allowing the user to save time, increase productivity, legal and regulatory compliance
Key success factors	Lessons learned
<ul style="list-style-type: none"> Support from upper management, business owners Training and awareness 	<ul style="list-style-type: none"> Users are receptive to change that make them more productive and helps the company Engaging all stakeholders from store owners to legal, IT, audit, privacy, record management, etc.

Data protection technologies – transaction & activity monitoring

Leading financial transactions processor	
Global Financial services firm	
Business problem / engagement type	Engagement duration
<ul style="list-style-type: none"> ▪ Large implementation to deliver highly flexible and scalable data integration layer. Meeting three key requirements: <ol style="list-style-type: none"> 1.Feed transaction data to real time settlement interface 2.Process incoming feeds into the system (i.e. member profiles, currency rates, account range data) 3.Provide outgoing feeds with data to clearing, billing, fraud reporting and other downstream systems 	<ul style="list-style-type: none"> ▪ Project duration: 36 months
Approach summary	
<ul style="list-style-type: none"> ▪ Deloitte provided business process, solution architecture and development expertise ▪ Assessed the existing environment (i.e., integration methods, data quality, data integration business rules) ▪ Defined the functional requirements and technical requirements ▪ Defined the future state data integration solution architecture based on Ab Initio 	<ul style="list-style-type: none"> ▪ Developed and tested the Ab Initio programs ▪ Supported the credit card transaction process system testing phases (e.g. SITs, UAT, PT, E2E testing) ▪ Supported post-production activities ▪ The data integration team worked collaboratively with the client and transitioned their role to the client’s support organization
Key success factors	Lessons learned
<ul style="list-style-type: none"> ▪ Support from upper management, business owners 	<ul style="list-style-type: none"> • Architect for scalability and performance, test to verify

Data protection technologies – data sanitization

Major Canadian bank	
Large Canadian organization	
Business problem / engagement type	
<ul style="list-style-type: none"> ▪ Aligning autonomous business units under a common corporate wide data obfuscation strategy ▪ Identifying current business and technology obfuscation activities and direction, determine the corporate vision and strategic goals, develop data obfuscation requirements, and then develop a roadmap that addressed both tactical and strategic recommendations that could be implemented to fully develop a data obfuscation solution 	
Approach summary	
<ul style="list-style-type: none"> ▪ Developed Total Cost of Ownership model of various components of the data obfuscation program implementation ▪ Current State Assessment—reviewed existing program documentation and assess the current obfuscation directives and recommended application inventory maintenance changes ▪ Data Obfuscation Best Practices—Conducted workshops to benchmark what other financial institutions are doing , and recommend successful practices and tactics 	<ul style="list-style-type: none"> ▪ Data Obfuscation Operating Model—recommended an operating model including roles and responsibilities, program governance, obfuscation framework lifecycle ▪ Strategic Roadmap— Addressing obfuscation deployment to protect sensitive customer data collected, stored, and used, based on application risk prioritization and proactive incident response for data breaches
Key success factors	Lessons learned
<ul style="list-style-type: none"> ▪ Solid business case helped support the obfuscation strategy, winning over project stakeholders 	<ul style="list-style-type: none"> ▪ Effectiveness of obfuscation program for controlling and mitigating risk

Why Deloitte?

- The largest Security & Privacy consulting capability in Canada with over 200 dedicated professionals across the country
- As a part of Enterprise Risk Services, we also have access to over 450 Canadian IT risk professionals
- A global IT Risk Management and Security & Privacy Services team of over 9,000 professionals
- Over 150 Certified Information Systems Security Professionals (CISSPs)
- Presence in 10 Canadian cities, with 4 Security Technology Centers (STCs) located strategically across the country
- Independent analysts consistently rate Deloitte as a global leader in the security consulting and technology risk management space
- Global alliances with market leading vendors

Questions?



For more information

If you would like more information about privacy and data protection or how Deloitte can help your organization, please contact one of the following professionals:

Adel Melek

Partner

(416) 601-6524

amelek@deloitte.ca

Andreas Faruki

Partner

(416) 601-4693

afaruki@deloitte.ca

Reza Kopae

Senior manager

(416) 601-5938

rkopae@deloitte.ca

Deloitte.

Next session

**Global Business Continuity
Management**

Date: November 20, 2008
RSVP: spwebcast@deloitte.ca

Deloitte.

Deloitte, one of Canada's leading professional services firms, provides audit, tax, consulting, and financial advisory services through more than 7,600 people in 56 offices. Deloitte operates in Québec as Samson Bélair/Deloitte & Touche s.e.n.c.r.l. The firm is dedicated to helping its clients and its people excel. Deloitte is the Canadian member firm of Deloitte Touche Tohmatsu.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, its member firms, and their respective subsidiaries and affiliates. As a Swiss Verein (association), neither Deloitte Touche Tohmatsu nor any of its member firms have any liability for each other's acts or omissions. Each of the member firms is a separate and independent legal entity operating under the names "Deloitte," "Deloitte & Touche," "Deloitte Touche Tohmatsu," or other related names. Services are provided by the member firms or their subsidiaries or affiliates and not by the Deloitte Touche Tohmatsu Verein.

© Deloitte & Touche LLP and affiliated entities.



Member of
Deloitte Touche Tohmatsu