

May 2009

Data Protection & Data Loss Prevention: Keeping sensitive data out of the wrong hands



The heart of the matter

Data security breaches pose a serious threat. Companies need to reduce risks associated with exposing customer data, losing intellectual property, or violating compliance obligations.

What data is at risk of exposure?

- Personally identifiable information, such as name, address, Identification number
- Personal medical information, such as medical history
- Customer financial information, such as credit card numbers, transactions history
- Intellectual property, such as product formulas, source code, research and development
- Strategic business information, such as customer trends, marketing strategies, mergers and acquisitions
- Legal or public relations information, such as lawsuits, failed product tests
- Security information, such as usernames and passwords

What risks does data theft pose for organizations?

- **Failure to comply with regulations**, which may result in stiff civil and financial penalties for organizations and their top executives
 - חוק הגנת הפרטיות התשמ"א
 - Sarbanes-Oxley Act (SOX)
 - Health Insurance Portability and Accountability Act (HIPAA)
 - Payment Card Industry (PCI)
 - EU Data Protection Directive
 - Gramm-Leach-Bliley Act (GLBA)
- **Loss of customer confidence** in the security of their data within the organization, which may result in customers terminating their relationships with the organization
- **Reputational damage**, which may result in diminished new customer acquisition and difficulty forming new partnerships with third parties
- **Loss of competitive advantage**, which may result from intellectual property becoming available to competitors or the general public
- **Response costs**, which, in the USA, according to the Ponemon Institute's 2008 annual study, average \$6.6 million per breach.
- **Decreased stock prices**, which may result from any of the risks above.

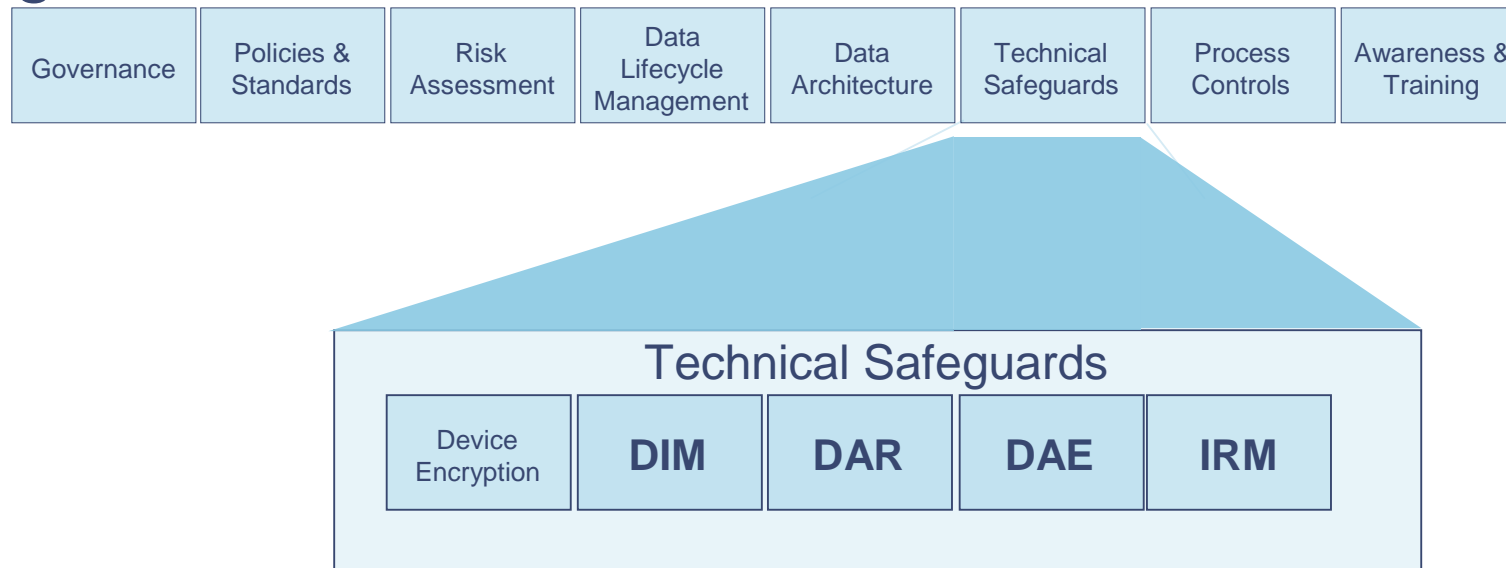
Which companies should be most concerned?

- Companies that are about to implement a **workforce reduction**, which may prompt malicious data theft by a disgruntled employee.
- Companies whose **employees regularly export data** from the customer relationship management system and send it, typically unencrypted, to their personal e-mail addresses so they can work from home companies whose cultures do not educate staff on securing data.
- Companies whose **employees are unaware of protecting data**. This can result in employees transferring sensitive data unencrypted to customers, contractors, or other external parties.
- Companies that are **too focused on cost cutting** that they choose low cost alternatives that do not adequately protect sensitive data.
- Companies who **don't know where their most sensitive data resides** across the enterprise and may not have the appropriate controls in place to prevent unauthorized access.

What Makes Up a Data Protection Program

Governance	Policies & Standards	Risk Assessment	Data Lifecycle Management	Data Architecture	Technical Safeguards	Process Controls	Awareness & Training
<p>Who has oversight for data protection? How do you ensure regulations are adhered to?</p>	<p>Are policies and standards defined? Are they integrated with HR, Security, Compliance policies & standards?</p>	<p>Are Data Protection issues embedded in IT, Vendor, Business Risk Assessments? Is there a mechanism to assess the data protection risk in new applications, systems, business offerings?</p>	<p>Is there a plan for handling data from creation, to classification, to modification, storage and destruction?</p>	<p>How do you define data? What controls are required for each data level?</p>	<p>What technologies are in place to protect data, monitor it, report on violations?</p>	<p>What do you do when an event occurs? Who should see what information? How do you handle new data types?</p>	<p>What educational plans are in place to bring individuals into the protection program?</p>

How Does Technology Fit Into a Data Protection Program



- Data in Motion – Network
- Data at Rest – Servers
- Data at the Endpoint – Laptop computers/mass media storage
- Info. Rights Management (IRM) – Protection beyond your borders

What are the greatest threats?

- Over 88% of all data breaches in 2008 involved incidents resulting from insider negligence
- Third-party data breaches were reported by 44% of respondents in 2008
- Lost laptops are the number one cause of data breaches, accounting for 35% of the total
- System failure is the number two cause of data breaches, accounting for 33% of the total

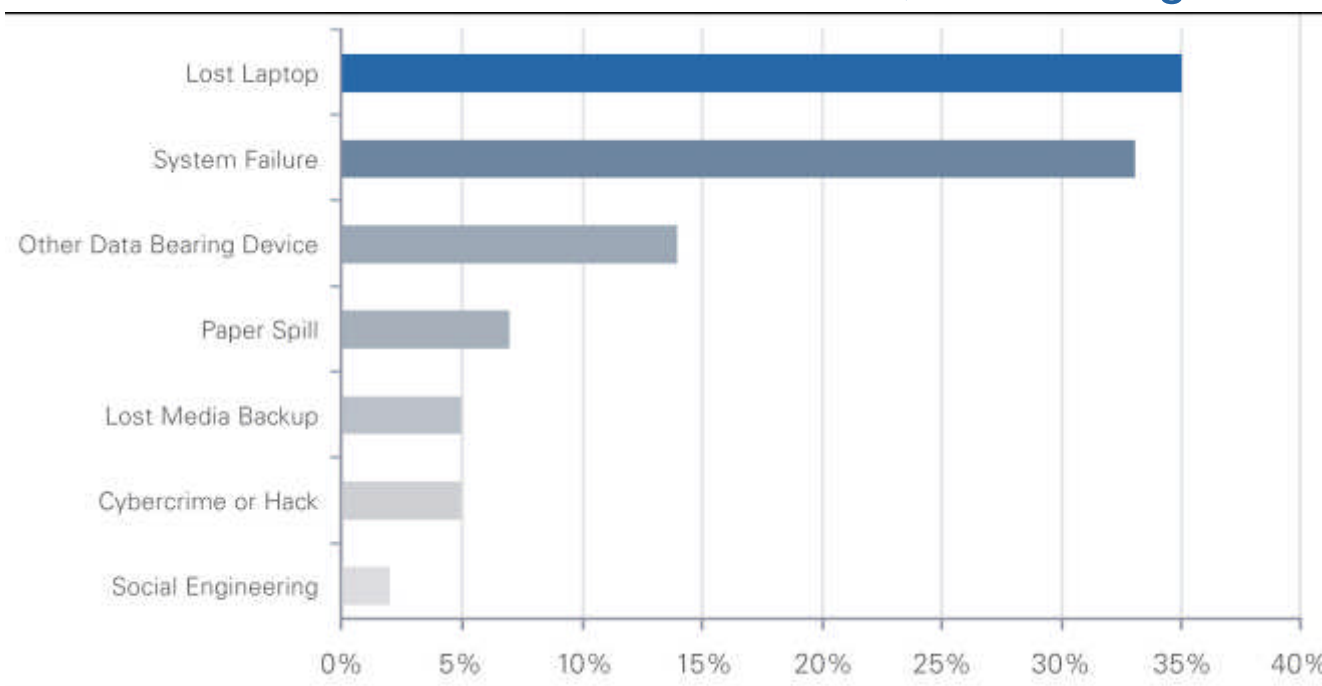


Diagram: 2008 Annual Study: Cost of a Data Breach – Ponemon Institute

Data Loss Prevention

What is Data Loss Prevention?

Data Loss: Any unauthorized disclosure of information resulting in compromised confidentiality of internal, proprietary or sensitive assets.

DLP can be used to monitor and/or prevent the unauthorized and unintended exit of data from an organization.

Although it can protect against some malicious activity, broken business processes and other unintended leaks are the true focus.

Other names:

- Data Leakage Protection
- Data Leakage Prevention
- Information Leak Detection & Prevention
- Content Monitoring and Filtering

How Mature Are Our Clients?

Dimension	Level 1 – Ad Hoc	Level 2 – Repeatable	Level 3 – Defined	Level 4 – Managed	Level 5 – Optimized
Strategy					
People					
Process					
Technology					

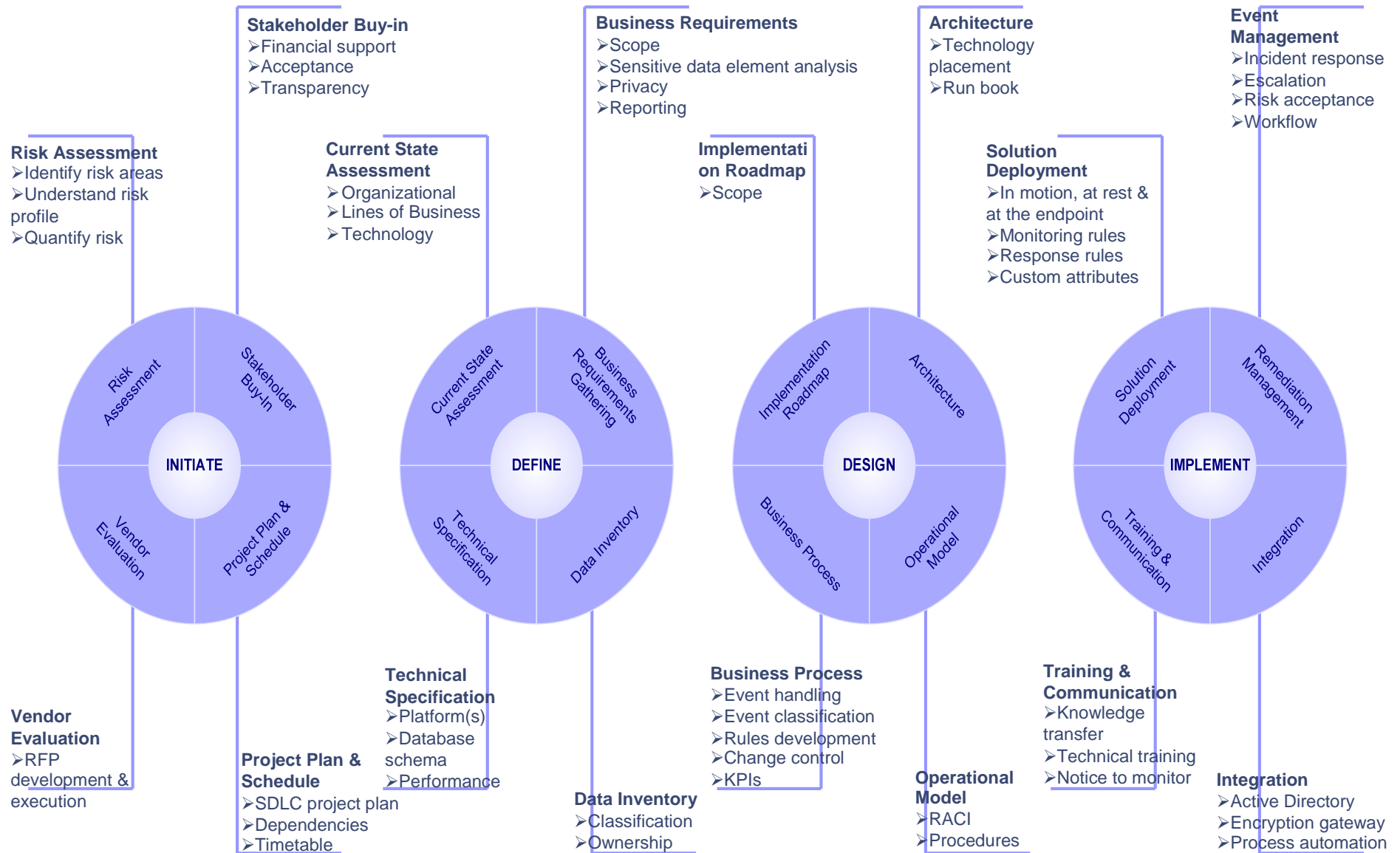
Where Should Organizations Be In the Near Future?

Dimension	Level 1 – Ad Hoc	Level 2 – Repeatable	Level 3 – Defined	Level 4 – Managed	Level 5 – Optimized
Strategy					
People					
Process					
Technology					

What you should be considering

- Where is the company's most sensitive data and who has access to it?
- What regulations and standards apply to the company's data?
- Do safeguards alert someone to ongoing security threats?
- Do employees, customers, and business partners understand their roles in protecting sensitive information?
- Do safeguards provide data with end-to-end protection, including mobile devices?
- Does a collaborative business model put the company's data at risk?
- What is the likelihood that the company has been a target of data and identity theft?

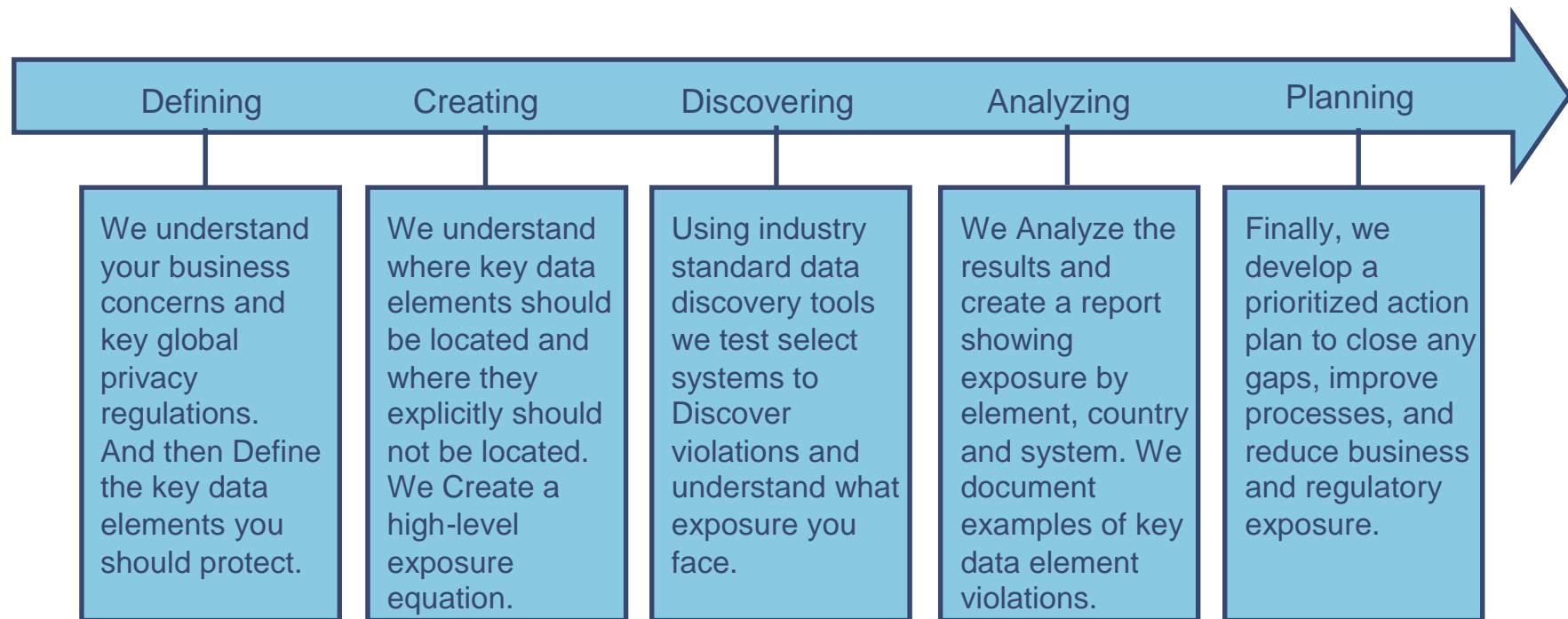
DLP Lifecycle



DLP Risk Assessment / Sensitive Information Assessment

Conducting a technical evaluation showing the actual unprotected data leaving our clients' network on the wire, the uncontrolled data in repositories or file shares, and unencrypted data on removable media, redacted to protect identity information and other sensitive data prior to review by privacy practitioners.

The Process



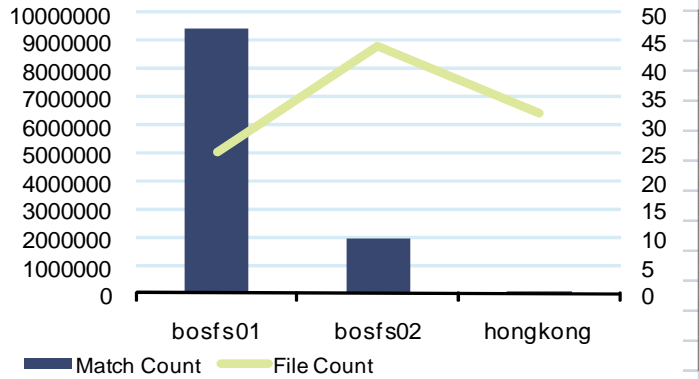
Sensitive Data Assessment Dashboard

Responsive Files: **101** Match Total: **11,416,676** Max: **2,251,326** Min: **1**

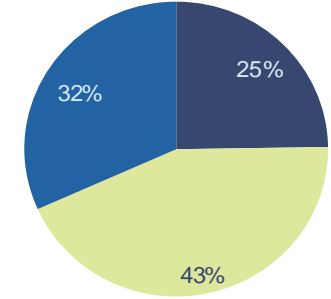
By File Server

Top 5 File Servers by Match Count

Server	Matches	Files
bosfs01	9,455,694	25
bosfs02	1,960,764	44
hongkong	218	32



File Count

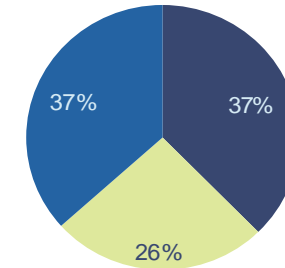
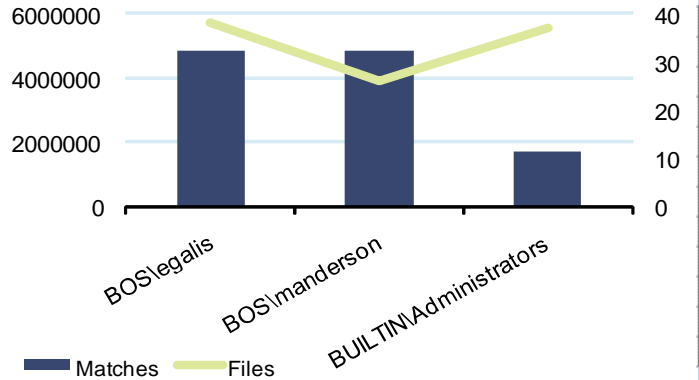


■ bosfs01 ■ bosfs02 ■ hongkong

By File Owner

Top 5 File Owners by Match Count

Owner	Matches	Files
BOS\legalis	4866111	38
BOS\manderson	4866028	26
BUILTIN\Administrators	1684537	37

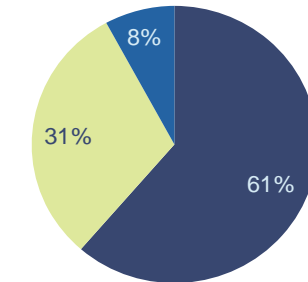
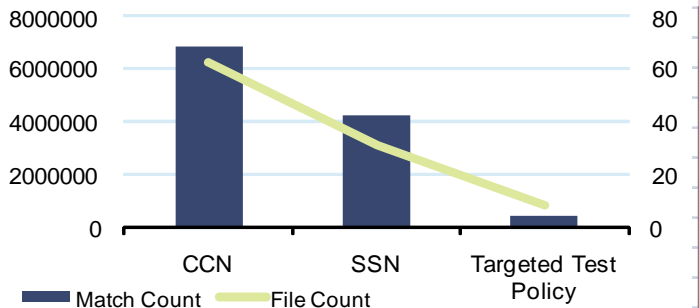


■ BOS\legalis
■ BOS\manderson
■ BUILTIN\Administrators

By File Policy

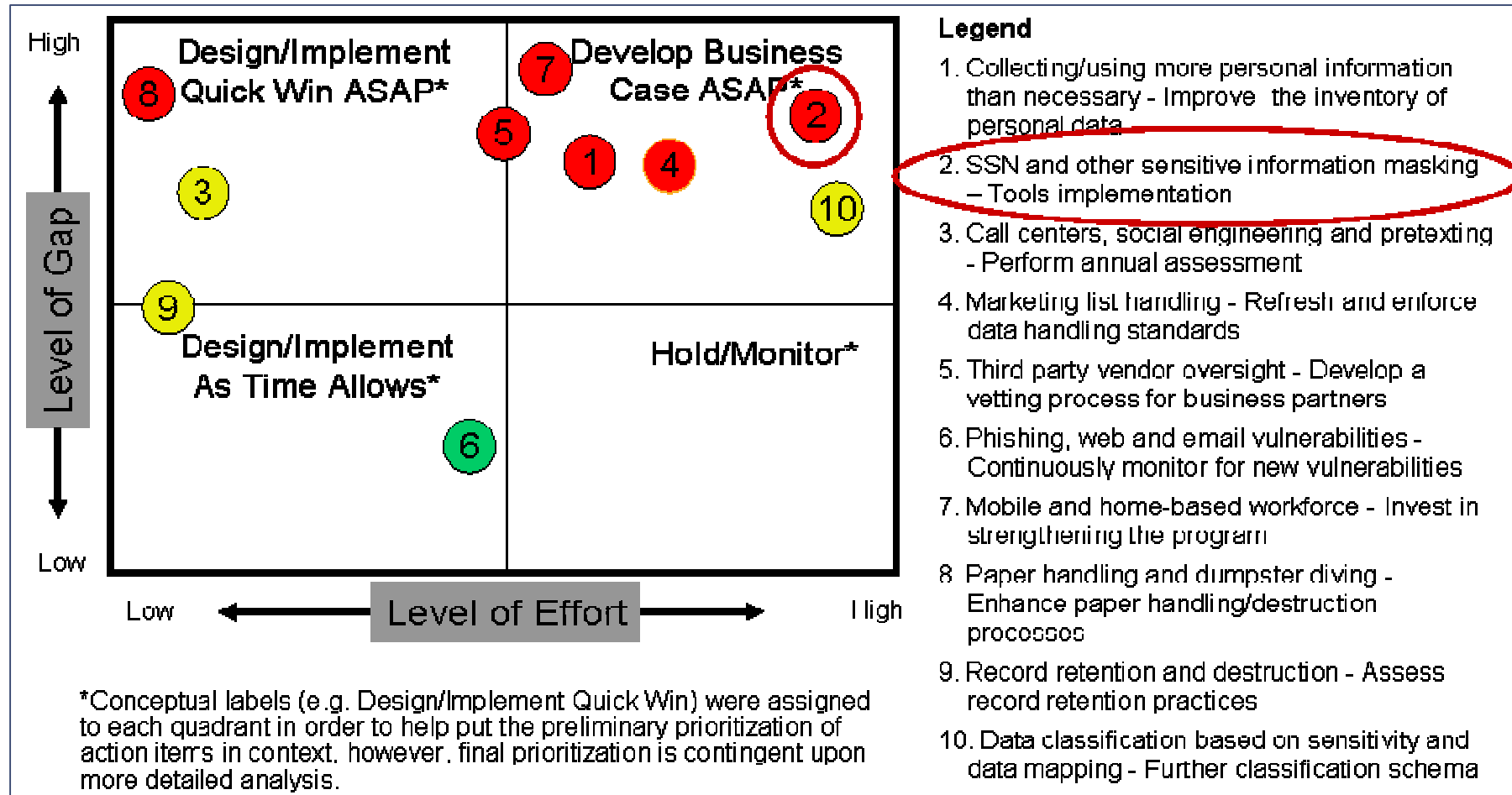
Top 5 Policies by Match Count

Policy	Matches	Files
CCN	6,828,122	62
SSN	4,187,754	31
Targeted Test Policy	400,800	8



■ CCN ■ SSN ■ Targeted Test Policy

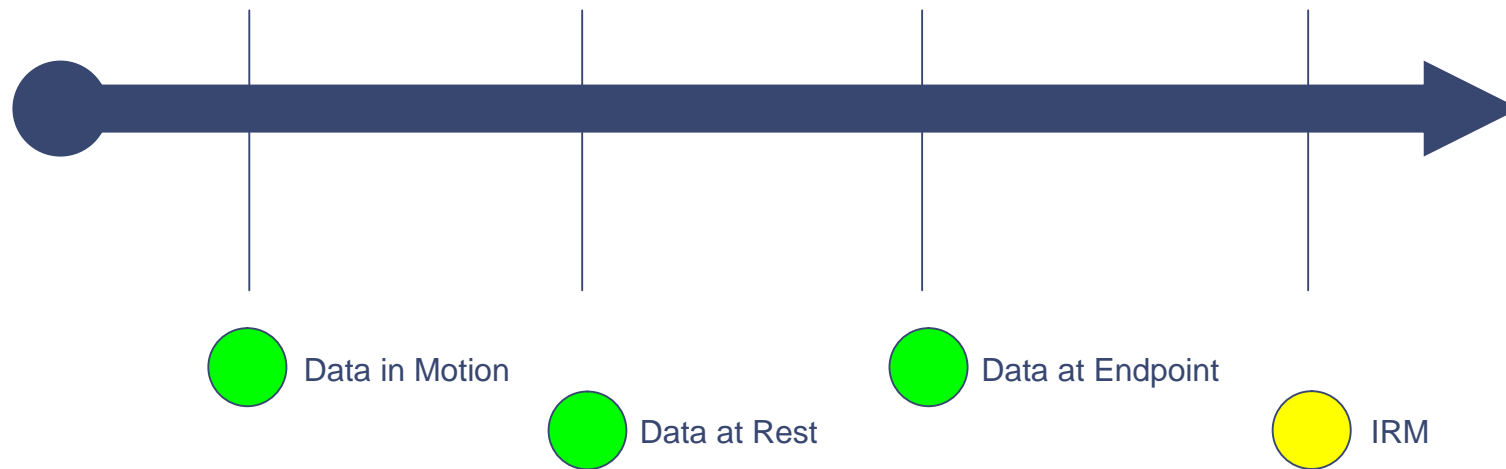
Example: Prioritized Action Plan



WHAT'S NEXT?



The Deployment Continuum Supports Graduated Roll-outs



- Data in Motion is typically deployed first because it requires no impact to end-user systems
- Data at Rest is deployed to examine data stores
- Finally, Data at Endpoint/IRM are deployed initially in limited roll-outs (i.e., legal, exec, security, etc.)
- IRM can be a near-term deployment option for those companies that have a very strong interest in protecting confidential data