
FORRESTER®

FORRESTER®

Состояние мирового рынка DLP в 2009 году

Билл Нагель
Аналитик
Forrester Research

2 октября 2009 г.


Securing mountains of data is a long, difficult, uphill struggle

Agenda

- About Forrester Research
- Forrester's view of data leak prevention
- The state of the DLP market
- Customer feedback on DLP
- Recommendations

Agenda

- **About Forrester Research**
- Forrester's view of data leak prevention
- The state of the DLP market
- Customer feedback on DLP
- Recommendations

About Forrester Research

- Providing advice on IT trends since 1983
- 2,500 client companies
- 1,000 employees (400 research professionals)
- Based in Boston (USA)
  - 5 research centers in US, 4 in Europe
- № 2 in global analyst marketplace
- Research, advisory, and consulting services
- Qualitative and quantitative research
  - Business Data Services surveys ca. 11,000 IT professionals every year

Security at Forrester

- 10 analysts cover security and risk management, including:
  - Application security
  - Data security
  - Governance, risk, and compliance
  - Identity and access management
  - Network security
  - Endpoint security
  - Security vendor strategy
  - Managed security services
  - Security strategy and performance

Agenda

- About Forrester Research
- **Forrester's view of data leak prevention**
- The state of the DLP market
- Customer feedback on DLP
- Recommendations

Definition: Data Leak Prevention

- Products that detect and optionally prevent violations to corporate polices regarding the use, storage, and transmission of sensitive information:
  - Financial information, such as cardholder data or bank details
  - Non-public personal information, such as government identifiers
  - Personal health information (PHI)
  - “Intellectual property,” such as earnings forecasts, product plans, legal documents, or confidential data

  Protected channels include e-mail, HTTP, FTP, file shares, copy and print, USB/portable media, databases and IM. Unlike access control technologies, DLP is *content-aware*.

Forrester regards endpoint *device control* technologies as complementary to, but distinct from, data leak prevention. But this may change.

Definition: DLP Lite

- Products that filter e-mail to detect transmission of sensitive information, which includes:
  - Financial information, such as cardholder data or bank details
  - Non-public personal information, such as government identifiers
  - Personal health information (PHI)

  DLP Lite filters content via regular expression, keywords and dictionary lookup.

  Protected channels are generally just e-mail and (less often) HTTP. Unlike DLP, DLP Lite by necessity filters content as a secondary task.

When is DLP the right (wrong) solution?

	Toxic data	Secrets
Creator/owner	• Business partners • Customers	• Enterprise
Relationship to data	Custodian	Owner
Examples	• Customer PII • Credit card numbers • Government identifiers	• Trade secrets • Strategic plans • Sales forecasts & financials
Source of value	External: determined by regulators and criminals	Internal
Compulsion to protect	Controlled by regulation, statute, or contract	Loss would cause strategic harm
Consequences	Cleanup, notification costs	Revenue losses
Key question	Why is the data circulating?	Who needs to know?
Priorities	•*Stop* circulation • Reduce use	•*Control* circulation • Reduce abuse
Product affinities	DLP, DLP Lite, encryption	DLP, ERM

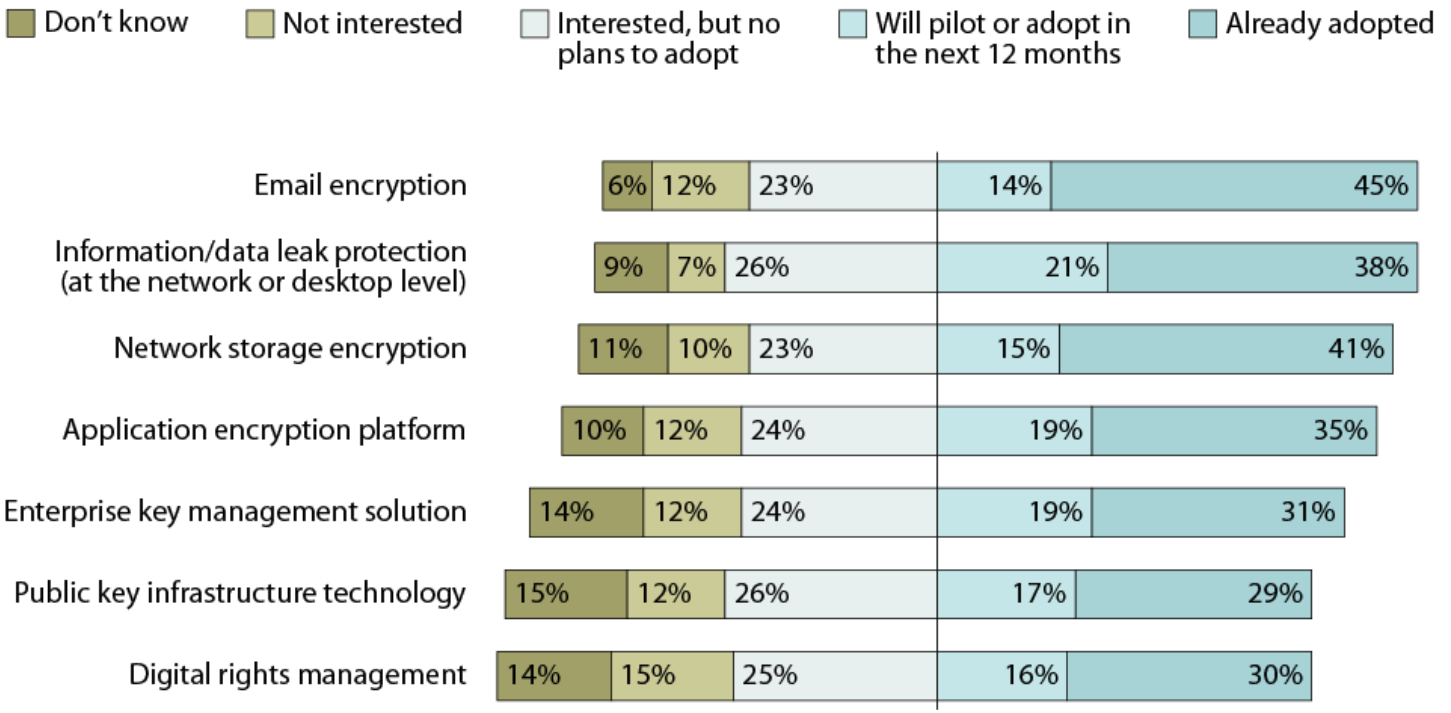
Agenda

- About Forrester Research
- Forrester's view of data leak prevention
- **The state of the DLP market**
- Customer feedback on DLP
- Recommendations

DLP is hot; ERM is not

About One-Fifth Of Firms Will Pilot Or Adopt Data Leak Prevention In The Next 12 Months

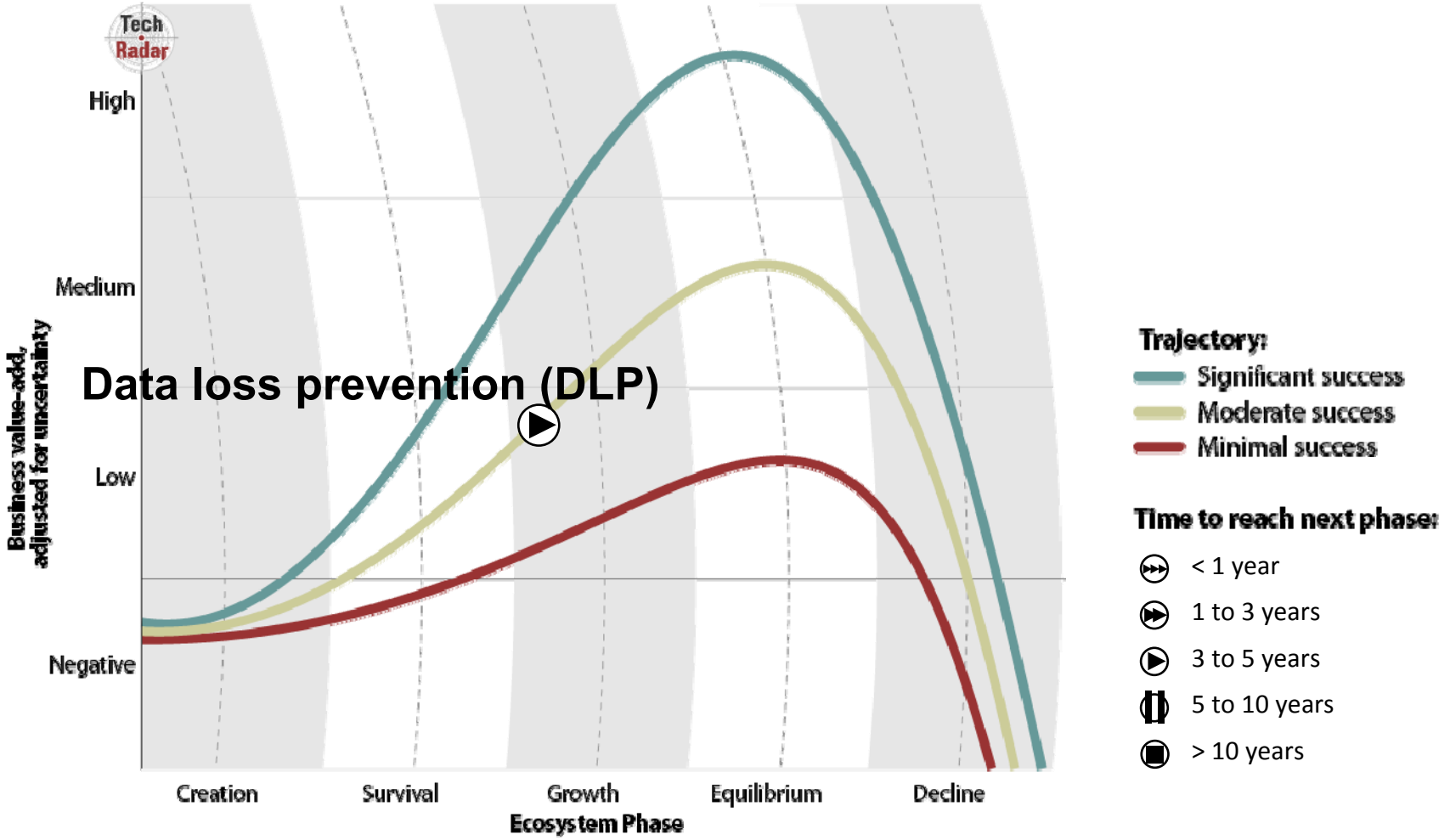
"What is you organization's interest in adopting each of the following data security technologies?"



Base: 881 North American and European enterprise IT security decision-makers who have data security challenges within their organization (percentages may not total 100 because of rounding)

Source: "The State of Enterprise Security: 2008 to 2009," December 2008.

DLP has entered the Growth phase of adoption

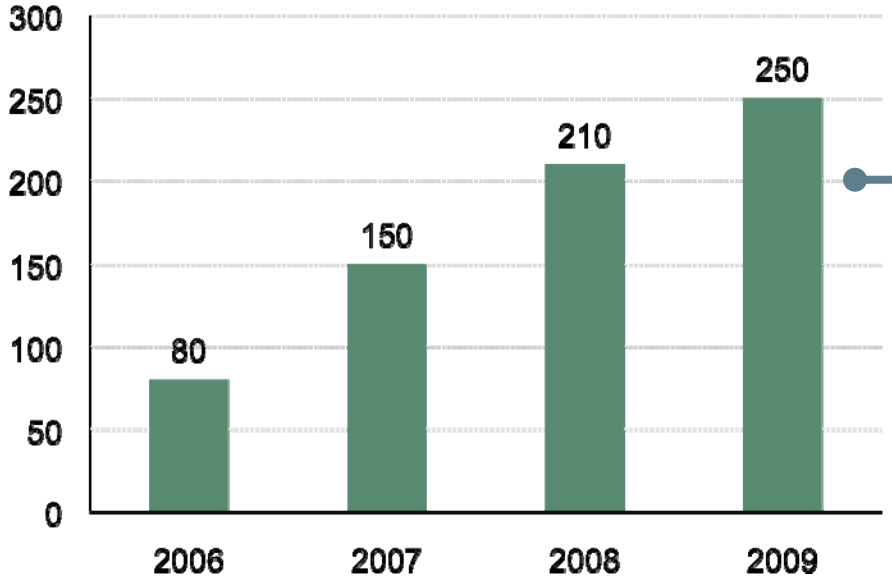


Why DLP is a growth-phase market

- DLP is clearly established as a market category
  - Customer awareness is extremely high
  - Weekly “toxic data spills” in newspapers
- DLP is a “checkbox” portfolio item for large security vendors…
  - Must have a DLP story
- …but not quite yet a checkbox item for customers
  - Network DLP adoption plans: 38% have it now; additional 21% will adopt in 2009
  - Desktop DLP: 15% have it now; additional 24% will adopt in 2009
  - DLP effectiveness hotly debated by some, e.g., the Black Hat crowd
  - DLP-Lite based on e-mail content filtering good enough for many
- Conclusion: DLP is a growth-phase market with potential for significant uptake and high business value

DLP product revenues ($m) and growth (%)

- Addressable base: between 1,500 and 2,500 customers
- Average deal size: between $100,000 and $200,000
- Strongest industries: financial and business services
- Strongest geography: North America (60+% of DLP market)
- Strongest by size: enterprises (1,000-4,999 employees)

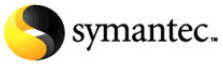


2009 growth assumption: 15-20%. Larger vendors will take outsized share as customers rank vendor stability as key selection criterion.

Sources: market estimates based on conversations with key vendors, resellers, and customers.

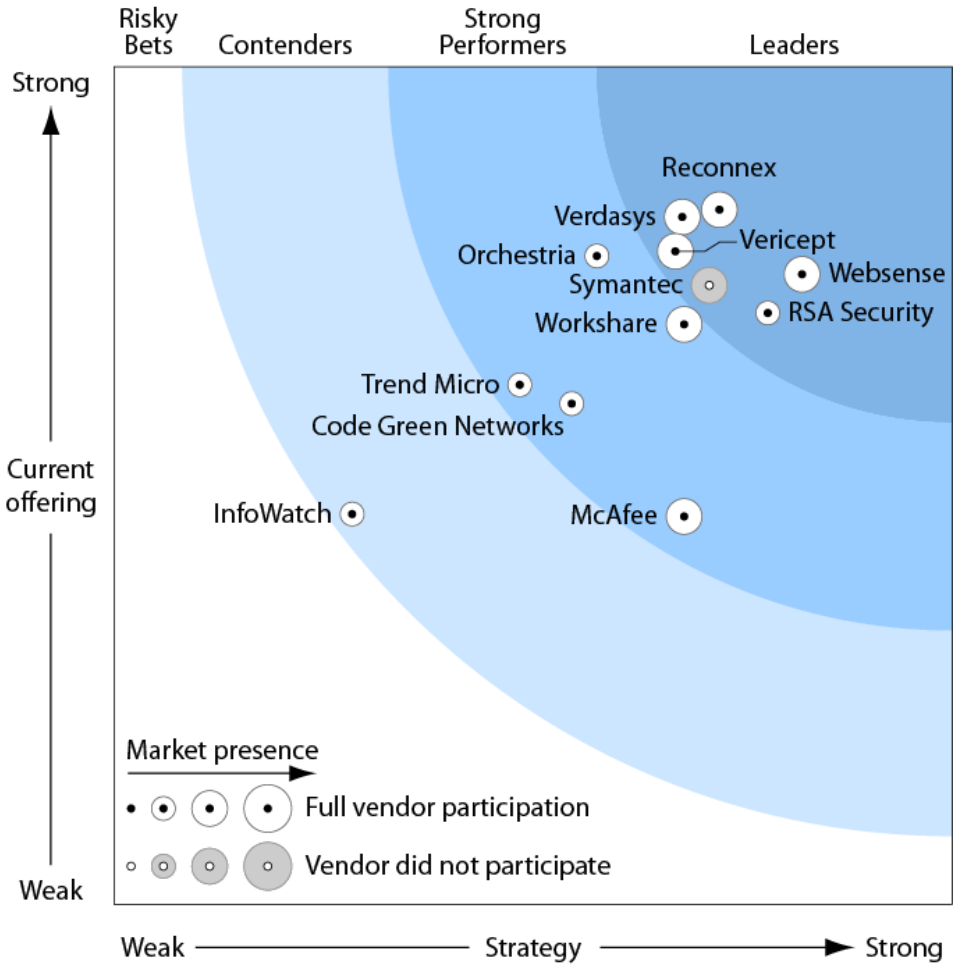
DLP vendor space: big, getting bigger (+ smaller)

Key Vendors



The Rest

2008's DLP Wave (vendor evaluation)



- Leaders
  - McAfee (Reconnex)
  - Symantec (Vontu)
  - Websense
  - RSA Security
  - Verdasys
  - Vericept
- Strong performers
  - CA (Orchestria)
  - Workshare
  - Trend Micro (Provilla)

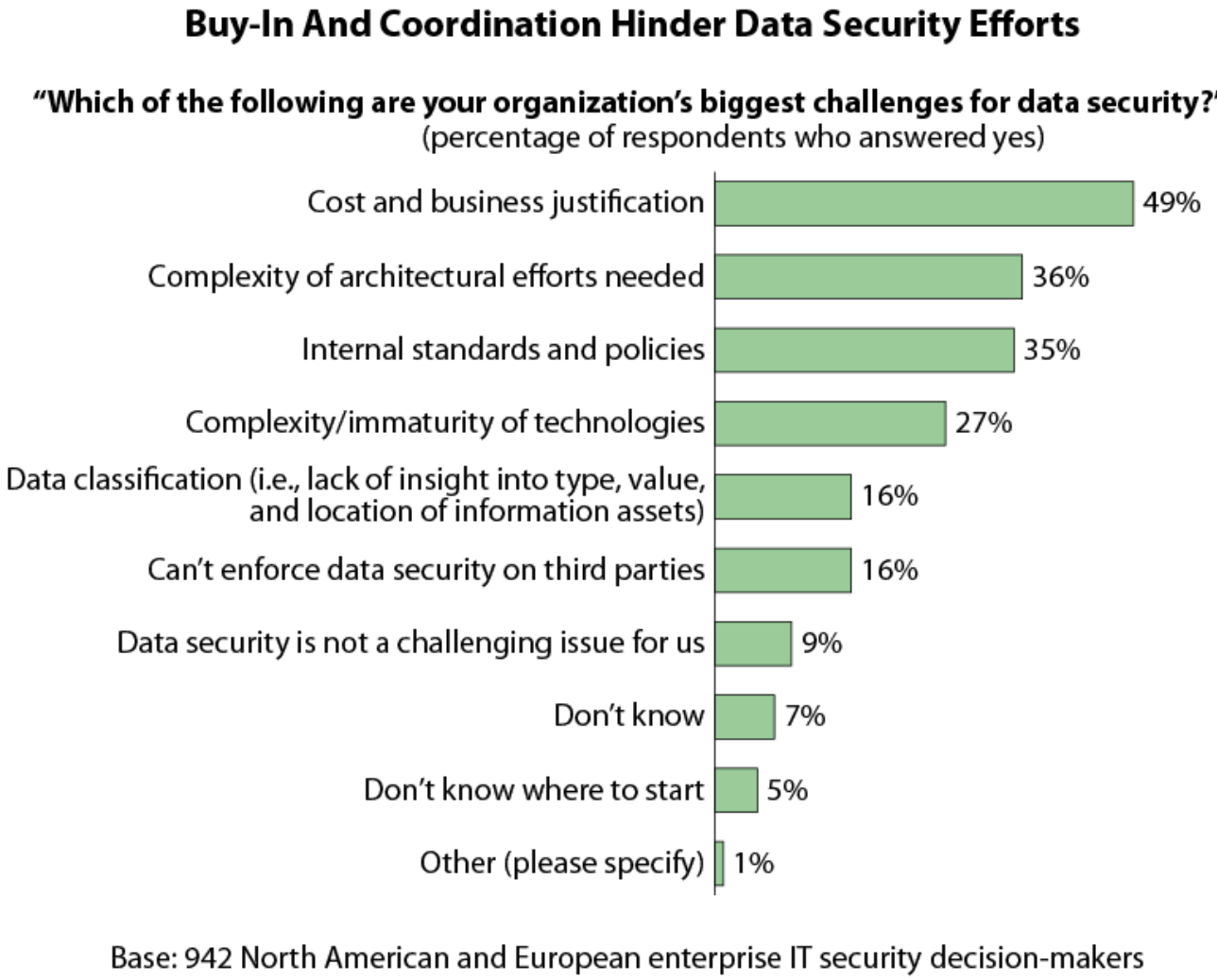
Competitive drivers

- Vendor imperatives driving desktop convergence
  - Massive consolidation; most independent DLP vendors snapped up
  - Larger vendors want to expand share of wallet (and desktop)
  - Symantec (Vontu): focusing on desktop agent
  - Microsoft: integrate RSA (Tablus) data classification into infrastructure
- Three distinct camps emerging
  - Infrastructure incrementalists: CA, Microsoft
    - Identity + infrastructure + DLP or DLP Lite + ERM
  - Information life-cyclers: Symantec, RSA
    - DLP + eDiscovery + SIEM
  - Threat-mongers: McAfee, Websense, Trend Micro, Sophos
    - DLP or DLP Lite + disk encryption
- Wildcards: IBM, Cisco, Microsoft

Agenda

- About Forrester Research
- Forrester's view of data leak prevention
- The state of the DLP market
- **Customer feedback on DLP**
- Recommendations

Clients: data security is a messy problem



Source: "The State of Enterprise Security: 2008 to 2009," December 2008.

But many are skeptical of standalone DLP

- "Digital information is meant to move."
- Information classification is not embedded into work processes
- Technical solutions are not standardized
- Recent experience with EMEA clients:
  - No CISO at the meeting were evaluating DLP products; only about 25% considering it
  - "DLP is an American idea. They're rules-based. We're principles-based. Technology isn't the answer here."
  - PCI is a big driver of DLP in the US. But EU has better security and privacy (e.g., chip+PIN)

Most implementers use few features

- Basic detection of toxic data: 75%+ of the uses
- Typical deployment path: DIM → Discover → DAR (planned)
- E-commerce user
  - "We use the PCI modules, for just two types of traffic: government IDs (SSNs) and credit card numbers. We are not using any other features because it's more than we can handle. [Too time-consuming]"
- Government user
  - "Did a good job finding SSNs and CC#s… We found challenges with other kinds of data. For example, if someone put into their e-mail footer 'this e-mail is sensitive or unclassified' we would get thousands of hits."
- Financial services user
  - "Right now, just the network monitor is in place. Excluding the database server. We have plans to activate the network discoverer by end of Q1. We plan to activate the endpoint discoverer by Q3."

Agenda

- About Forrester Research
- Forrester's view of data leak prevention
- The state of the DLP market
- Customer feedback on DLP
- **Recommendations**

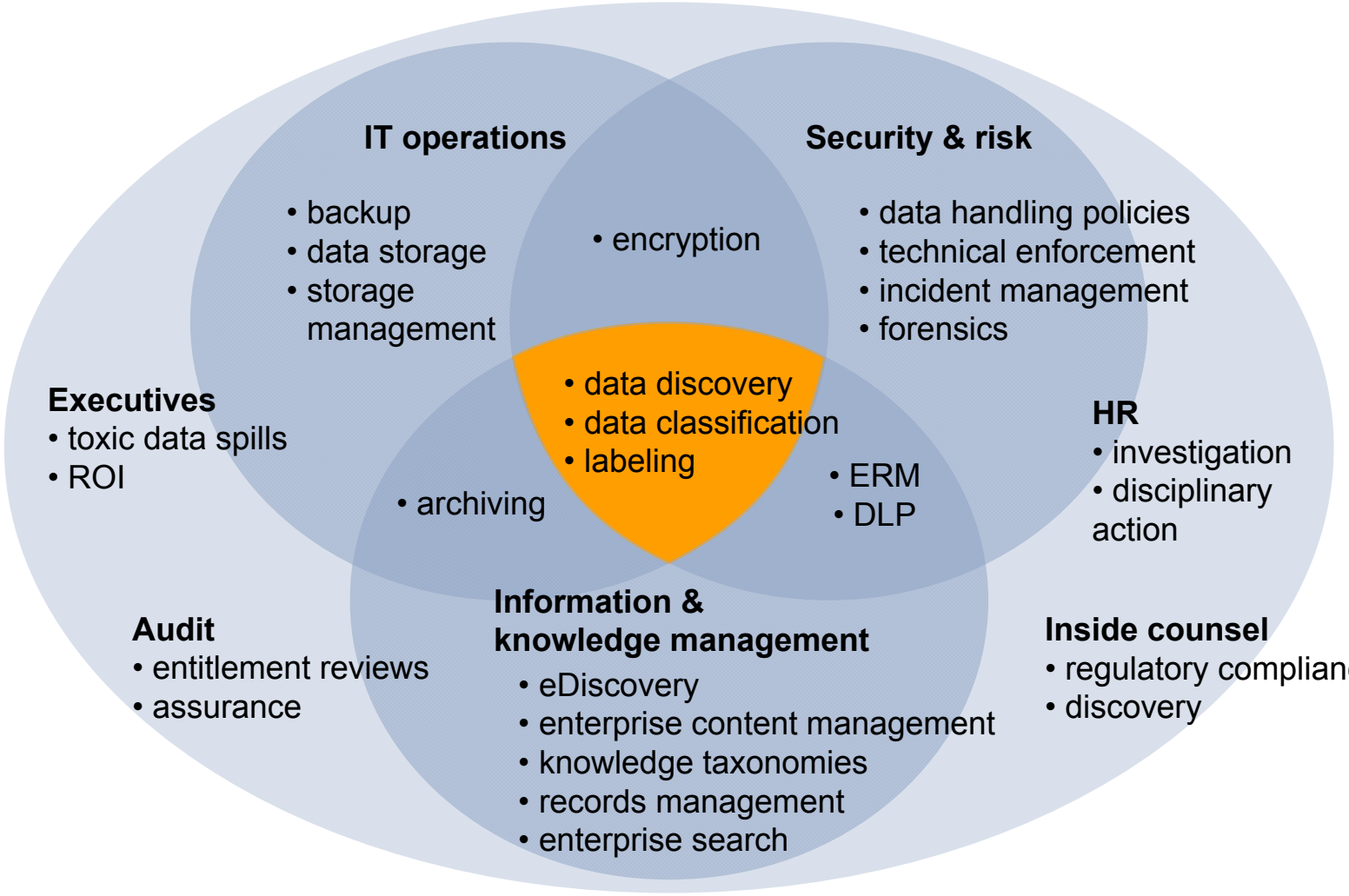
Peer advice: the importance of process

- **Start small**. “Be specific as possible, start slow. We started with a very specific problem: where is credit card information moving from or to on [our systems]?”
- **Get everyone involved**. “Before deploying the product: put a streamlined process chain in place… We have an investigator who reports to the CSO. They have a line to legal, HR, and audit. The steering committee has members from legal, HR, audit, security. One of the reasons it took so long to deploy was because we wanted to get the process stuff ironed out.”
- **Use findings to improve processes**. “Get a lot of people involved. Get as many examples of data as you can, and get the product to use exact data matching for that. Also, don't turn on preventative measures for at least 6-9 months. Use the findings as a reason to go back to process owners and try to fix the process.”

Keys to success: the “Six P’s” of DLP

Priorities	• Start with the highest-value data types first
Process	• Classification, incident detection, and escalation; “broken” processes
Partners	• HR, legal, IT ops, compliance, business units
Precision	• Be specific about data types, and owners. • Use examples to improve the process
Patience	• Cultural change; technology time-to-value
Privacy	• Local rules and regulations • Infrastructure segregation

Success requires cross-functional participation



Recommendations: data-centric security

- Take ownership for basic data security tools
  - Full-disk encryption, terminal services
- Business units (not IT security) should drive initiatives to protect business data – and be accountable
  - Name the exact business content requiring tough security
  - You can't protect everything – so be smart
- Rethink how users work
  - Move responsibility from user education to inescapable automatic controls (not bans!)
- IT security should only be responsible for deploying data protection technologies requiring minimal customization

Спасибо большое

Bill Nagel

+31 20 305 4381

bnagel@forrester.com

www.forrester.com

Selected Forrester research

- December 2009, Forrester Wave™ "Data Leak Prevention, Q4 2009" *(in progress)*
- February 10, 2009, Inquiry Spotlight "Data Leak Prevention, Q1 2009"
- January 9, 2009, Trends "Top Data Security Predictions For 2009"
- January 5, 2009, Trends "Data-Centric Security Requires Devolution, Not A Revolution"
- June 6, 2008, Forrester Wave™ "Data Leak Prevention, Q2 2008"