



CRAFTING A SUCCESSFUL DLP PROGRAM

A HOLISTIC
APPROACH



INFOLOCK

CHALLENGES TO DLP SUCCESS

GOVERNANCE

STAFFING

TUNING

INCIDENT
RESPONSE

CHALLENGES TO DLP SUCCESS

GOVERNANCE

STAFFING

TUNING

INCIDENT
RESPONSE

GOVERNANCE

PROGRAM
OWNERSHIP

ACTIVE
DECISION
MAKING

GOVERNANCE

THE CHALLENGE:

Program ownership

Establishing core
stakeholders & those
responsible for driving DLP

THE APPROACH

- Start with those in InfoSec, IT, Risk & Compliance, Legal
- As DLP becomes more established, build outward toward key lines of business that work with sensitive data
- Hold regular meetings to discuss progress and keep members involved

GOVERNANCE

THE CHALLENGE:

Decision making

Adopting a risk-oriented
mindset for decision making

THE APPROACH

- Prioritize, start with DLP decisions that
 - Reduce the most amount of risk – for example, providing DLP protection for email
 - Introduce the least amount of risk to DLP – for example, white listing or automating the remediation of verified trusted business partners and processes in DLP

STAFFING

THE CHALLENGE:

Personnel

Lack of technical, IR, and
programmatic manpower &
expertise

THE APPROACH

- Cultivate internally – hire and designate the right people from your own staff
- Outsource – research and hire a vendor who can provide a comprehensive management solution
- Hybrid – build some staff internally, contract strategic consultative resources

TUNING

THE CHALLENGE:

Effective Tuning

Tuning DLP policies
effectively to reduce noise,
without introducing
significant risk

THE APPROACH

- Don't cast too wide of a net to start – if using broad patterns, use keywords and other validators
- Identify trusted business partners and approved business processes upfront, then build those into policies
- Leverage your own data sources with advanced DLP detection technologies

INCIDENT RESPONSE

THE CHALLENGE:

Incident Overload

Designing a workflow to
efficiently deal with incident
triage and remediation

THE APPROACH

- Divide incident response responsibilities into at least two levels
- Tackle highest severity incidents first
- Use built-in capabilities of the solution to aid in automation of workflow
- Bring insights learned in IR process back to policies

KEY TAKEAWAYS

- DLP should be a program, not a point security solution
- People and expertise are key to success
- Prioritize, especially risk reduction
- Develop a program plan & document it



CRAFTING A SUCCESSFUL DLP PROGRAM

A HOLISTIC
APPROACH



INFOLOCK