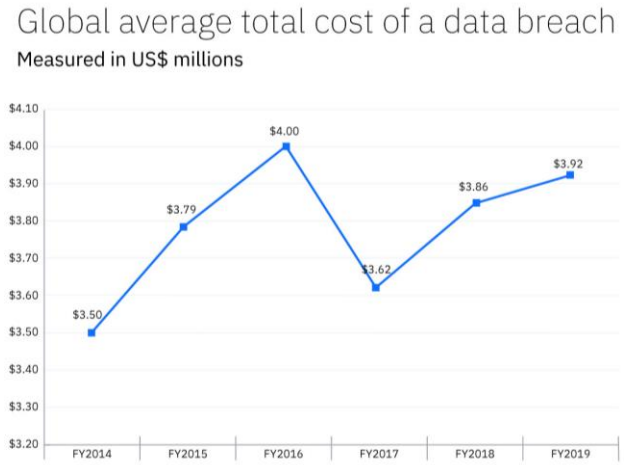
Asset Protection

Information can be a vital corporate asset. In additional to reputational impact, financial costs of data leakage can be significant. On average, the cost is $150 per record averaging $3.9 million per breach.[i] This figure can be double for highly regulated industries or if the incident receives press attention.[ii]



Information assets shared by customers and other individuals require even greater protection. Personally Identifiable Information (PII), Protected Health Information (PHI), or payment card information (PCI) is generally suject to regulations with the potential for very stiff penalties.

Corporate assets require protection via a risk management approach.

- Business focused
- Risk management techniques
- Cost / risk alignment
- Technology as an enabler

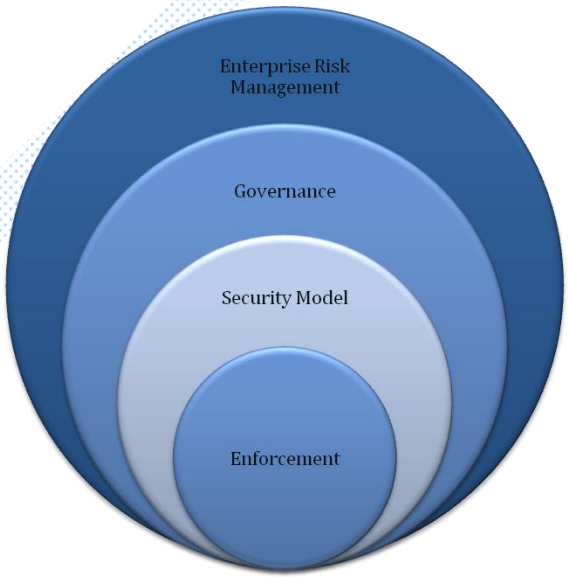
Risk Management

Risk management involves determining acceptable levels of risk for organizational assets. This assessment must come from business leaders and operational stakeholders. Constructing a business-driven model maps assets to key risk drivers.

Protection against external threats is important as malicious attacks constitute 51% of data breaches. However, 24% percent of data loss is caused by human error from insiders such as employees or contractors directly spilling data. System issues represent 25% of data breaches.[iii]

The root cause exposing this data tells a slightly different story. Most incidents do not occur because of nefarious intent from trusted parties, but rather from unintentional mistakes and misunderstood policies. This includes indirect spills from trusted insiders inadvertently exposing the organization to malicious external attacks. Surveys found that 63[iv] to 64% of all data breaches were a result of an internal root cause.[v]

Enterprise Risk Management



DLP should fit into a larger risk management model.

- ERM includes internal risk management and regulatory and compliance needs
- Governance creates and sustains data ownership and stewardship
- The security model includes the implementation framework that covers people and processes
- Enforcement includes the technologies used to implement the model and provide ongoing monitoring

DLP should be consistent with overall ERM with respect to policies, processes and practices. DLP should not diverge from ERM but extend it to encompass the exfiltration of relevant data assets.

Business Impact

Implementing DLP as part of a larger risk management program will yield a positive business impact. The business will have a mature risk management model that protects vital information assets.

- Discovered and classified information assets
- Established and consistent policies for data
- Automated enforcement of data protection policies
- Effective measurement of governance
- Formal documentation, awareness and training
- Proactive approach to managing risk

Enterprise Risk Management and DLP should not impede the business. While controls must be put into place, the impact on people and processes should be minimized. For example:

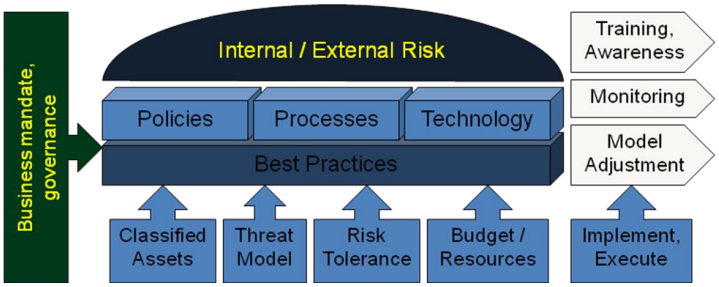
- Customer transactions must continue to flow smoothly
- Partners and distributors should be granted trust only to the extent they require provided their risk management controls meet or exceed client standards
- Operational overhead should be minimized and controls should not be so onerous as to encourage bypassing them
- Compliance and audit should be armed with effective tools and useful information so as to limit disruption to ongoing business

Data Loss Prevention Model

Creating a model makes prevention possible through:

policies + processes + practices + people

Technology is an enabler but does not provide prevention on its own. The following is a conceptual model of DLP as it fits into risk management.



To be effective, technology must:

- Align to organizational policies
- Implement efficient processes
- Utilize and support best practices
- Meet the needs of stakeholders and support their requirements

Data at rest, in use (screen scraping, etc.) and in flight must all be protected if the assets are at risk. Fortunately, technologies exist for all these states of data. The challenge is to develop the appropriate model and adjust it in response to monitoring and changes in the asset pool.

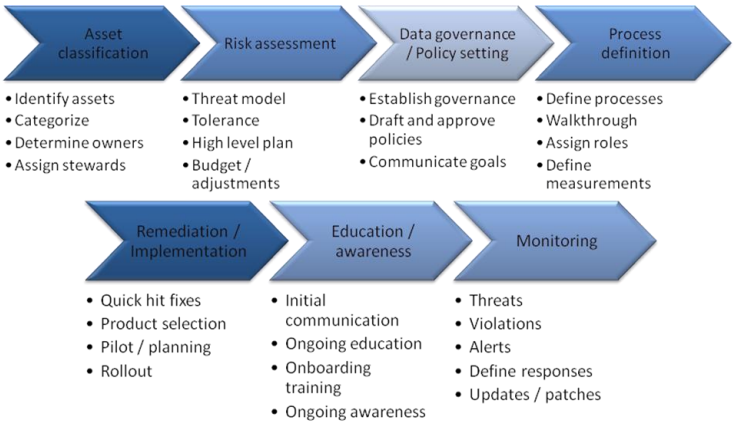
Results

A successful DLP engagement results in a sustainable model.

- Effective Policies Set: Crisp and meaningful
- Processes: Lean and measurable
- People: Right stakeholders involved
- Technology: Aligned to the business problem

Engagement Structure

Actionable Strategies defines a pragmatic approach for each client. A sample end-to-end engagement roadmap is depicted below.



For specific details on how we can help you plan and execute a Data Loss Prevention program, please contact your Account Manager.

---

[i] Ponemon Institute, *Cost of a Data Breach Report*, 2019

[ii] Ernst and Young, *Insights on governance, risk and compliance*, 2011

[iii] Ibid.

[iv] Apricorn, *2019 Survey*

[v] Verizon, *Data Breach Investigations Report*, 2019