www.pwc.ru

Business Drivers – the key difference between success and failure for DLP

Christopher Gould

28 October 2011

pwc

DLP? Or should it be ILP?

"When talking to stakeholders in our businesses what is meaningful to them – data or **information**?"

We need to consider the real challenges to implementing a DLP/ILP solution…

- Finding a common language between business and IT
- Failing to understand the capabilities (and limitations) of the tools
- Integrating the tools into existing processes
- Determining an appropriate risk tolerance level
- Defining simple and reusable information classification levels
- Building an accurate and appropriate information asset inventory
- Turning business problems into technical requirements
- Developing appropriate response and enforcement options

For a firewall implementation we may not think about involving our sales team, but this is different

These are business challenges and mean we need to involve and not alienate them…

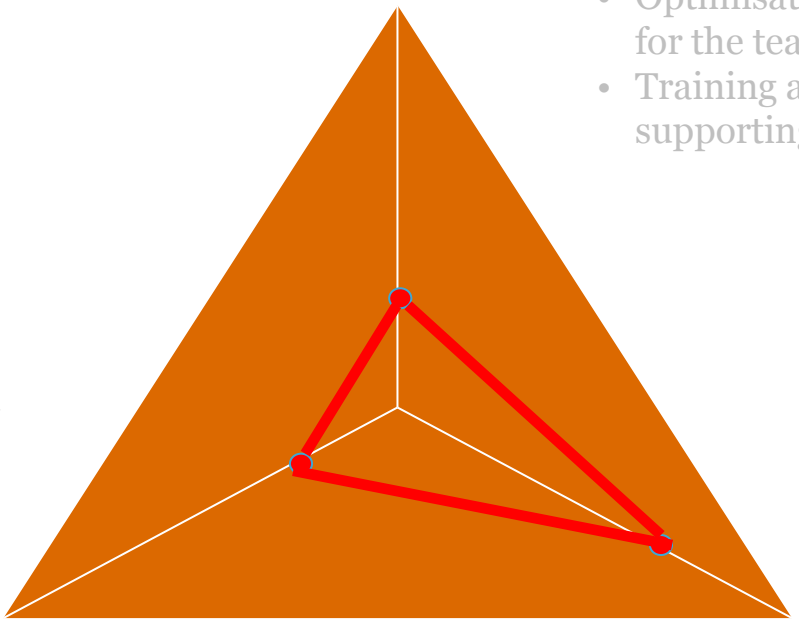
- Consider appropriate enforcement mechanisms (monitor first)
- Avoid ‘covert’ implementation
- Think about user overhead
- Consider ‘legitimate uses’ which cause false positives
- Validate the ‘registered data’
- Consider how we ‘identify offenders’
- Solicit regular feedback from the business

If business understands the what, why, how and when we have a bigger chance of success…

The challenge is to evolve our thinking from one focused on the 'technology solutions'

People

- Clear accountability and role clarity
- Optimisation of resource allocations for the team
- Training and development supporting the resources



Process

- Simplified and standardised Frameworks
- Change management capability
- Internal and industry best practice

Technology

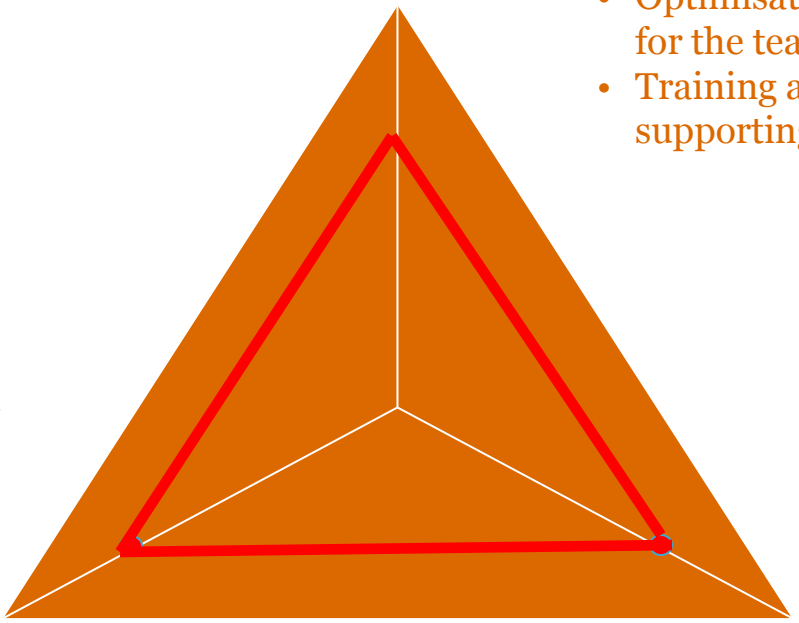
- Leverage technology through common tools tied to standard processes
- Organisational knowledge bases being used

Which is an approach that has a low probability of long term success…

To a thinking that is focused on the business problem we are trying to solve…

People

- Clear accountability and role clarity
- Optimisation of resource allocations for the team
- Training and development supporting the resources



Process

- Simplified and standardised Frameworks
- Change management capability
- Internal and industry best practice

Technology

- Leverage technology through common tools tied to standard processes
- Organisational knowledge bases being used

Which is more likely to have credibility, longevity and provide a solution that really protects information

Building effective DLP framework based on real world cases…

Case 1: Global universal bank

Case 2: Global gaming and leisure company

Case 3: Large professional services firm

Why choose these examples?

- All have regulatory requirements they need to consider
- All have confidential and proprietary data included in the scope
- Different maturities of information security
- Their implementations are considered successful by the business users

- A high level of business engagement throughout the project

These

What are the common themes

"What do all these companies do right?"

A single, global and standardised baseline for ILP with support from an appropriate governance model…

- Greater alignment and standardisation in the execution of global Information Security objectives across regions
- An effective governance model to enhance the effectiveness of the global security function
- Consolidated view of what information types are held in and how it is handled across the information lifecycle
- A comprehensive records management system which considers not just confidentiality but also other requirements
- Clear roles and responsibilities from the board downward
- Pilot project to gain initial management buy in

There is a need to tightly define, document, communicate and embed accountability and responsibility for ILP

Tone at the top and support for the project from implementation continued through current operation…

Shift from a reactive to a proactive and risk based security posture…

- An effective global ILP framework which maps to each of the cases wider strategic objectives and industry good practice
- Focus is on strategic initiatives rather than “firefighting”
- Hands on involvement and ongoing support from the business
- Clear understanding of accountability and escalation for 3rd parties

There is a need for a target framework to support effective cross-functional and global operations

There is a need to address increased outsourcing and third party relationships

Data loss incidents not only impact our business, but also have potential impacts on others…

Data classification expertise driven centrally that defines the information types that require protection and associated handling and management requirements…

- Inventory of critical information assets clearly defined including but not limited to client data, M&A related information, strategic marketing and investment information and personal data
- Clear guidelines to assist the business in appropriately classify information
- Use existing legislation and regulations as **guidance** to develop the schema
- Independent review that classification is appropriate

There is a need to clearly understand all information assets globally and the associated risks to determine appropriate classification and handling requirements

Simple, clear and well communicated models are more effective in the long term…

Security controls and activities remain stable and continue to operate effectively…

- Ensuring controls remain fit for purpose to protect the business
- Enhancement and efficiency opportunities will be identified
- Monitor and review mode kept open t allow business to have sustainable, repeatable control that is not onerous
- As much as possible the operation of the ILP framework should be transparent

The extent to which changes to frameworks requires a change to current security controls and activities will need to be addressed. Need to ensure that any solutions deployed have minimal impact to business as usual operations

We are still here to support the business, not to stop the business…

Awareness and communications to be centralised and drive a security aware culture…

- Regional security managers on the ground to raise awareness and respond to challenges
- Brining security “front-of-mind” and into business as usual processes
- Continued user awareness and training at all levels and be very aware of the culture that exists
- KPIs built into compensation and reward system that reflect the importance of protecting information

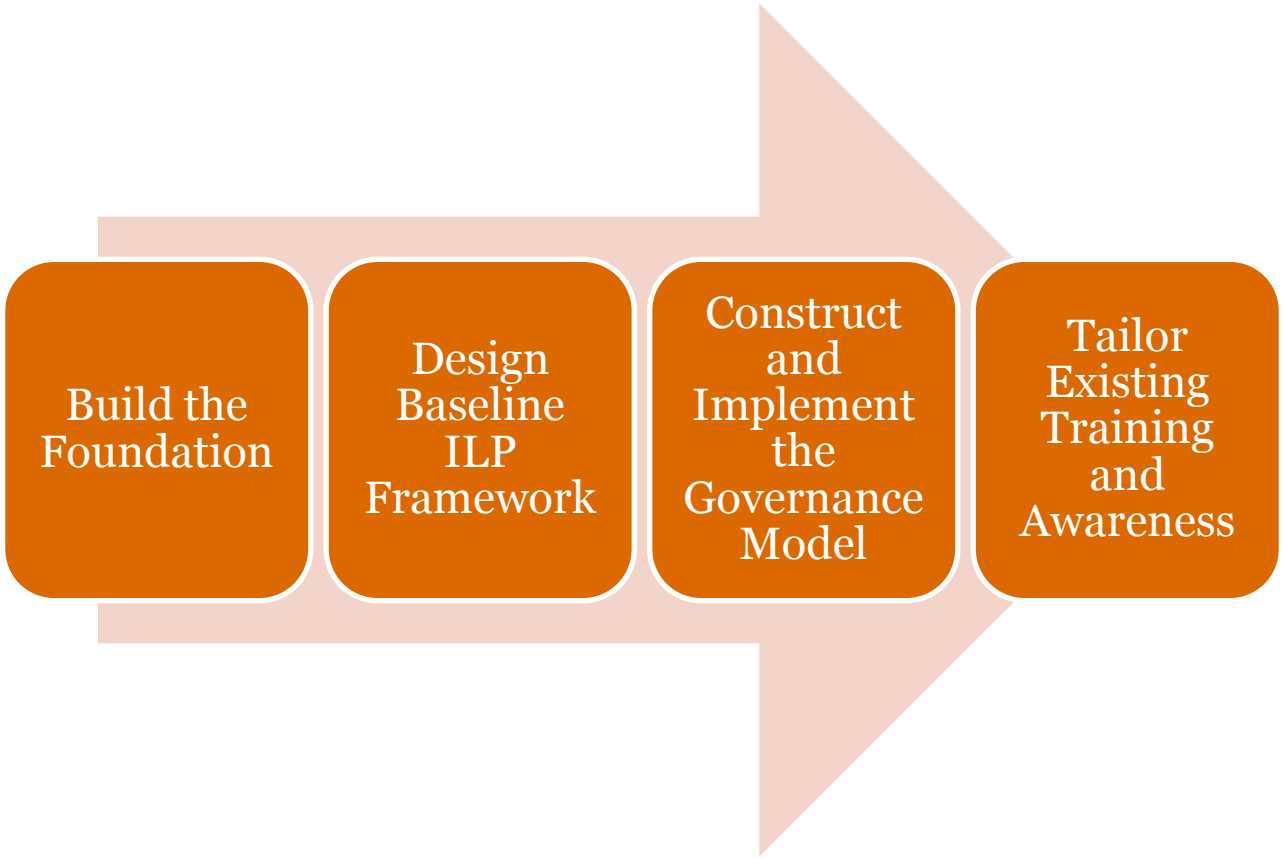
There is a need to define and appropriate roles, responsibilities and information handling requirements commensurate with data classification

Legitimate access to information does not grant the right to take it out of the company…

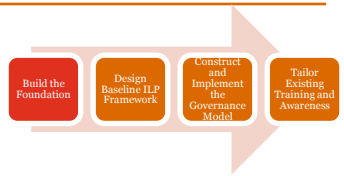
If we put this together, we can build an approach for successful ILP

"Lessons learned by others are a good source of learning for ourselves"

Our approach

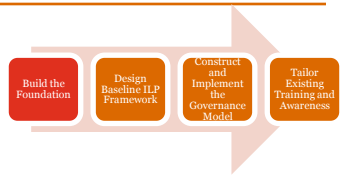


Build the foundation



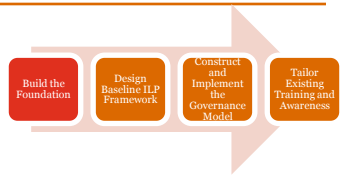
- Clearly defined and agreed data classification scheme in line with risk appetite.
- Standardised information handling requirements based on classification levels
- Baseline requirements for information asset management
- Simpler, standardised and more robust processes
- Clear understanding of regulatory requirements

Design Baseline ILP Framework



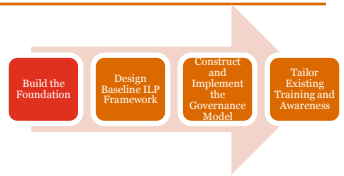
- Define a global baseline DLP requirements that identifies:
- Policy
- Supporting processes and procedures
- Information types
- Incident response procedures
- Technology baseline requirements
- Ability to share and collaborate knowledge and best practices

Construct and Implement the Governance Model



- Ensure effectiveness of the function by:
- Well defined organizational structure and role of 3rd Parties in governance and control
- Ability to share and collaborate knowledge and best practices
- Clear governance process enabled control
- Standardized global definitions
- Controls remain fit for purpose

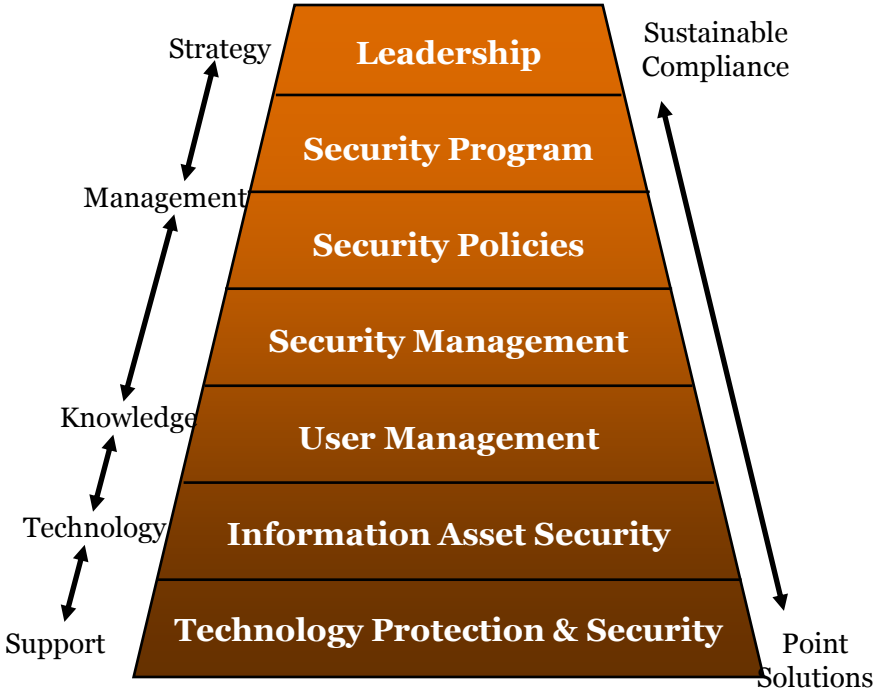
Tailor Existing Training and Awareness



- Successful adoption of Information Security governance:
  - clear governance process enabled control
  - standardized global definitions
  - controls remain fit for purpose
  - relevant KPIs for managers (and staff)
- Regular training and awareness including campaigns

In summary the fundamental approach needs to be a top down view starting with risk…

- Sustainable security needs to be driven from leadership based on risk
- Individual point solutions may seem to provide quick wins, but will eventually be more costly in the long-term
- Despite vendor promises, technology solutions only provide part of the solution for any compliance
- Complex and competing compliance requirements require management and strategic vision and decisions
- Security is not a tool, it is a process and a requires a robust and well tested management approach to be successful



Unless we get it right at the beginning we will fight an uphill battle embedding ILP into our organization…

Without business involvement, DLP is not a business solution…

"There is no magic fairy dust that we can sprinkle on our infrastructure to make it secure

There is no magic wand we can wave to make all our people do the right thing

Technology based tools are the closest thing we have to magic, but they can't do it all by themselves…"

Focus on the risks and compliance will follow…

Christopher Gould
Director
Tel.: +7 (495) 967 6000
E-mail: christopher.gould@ru.pwc.com