



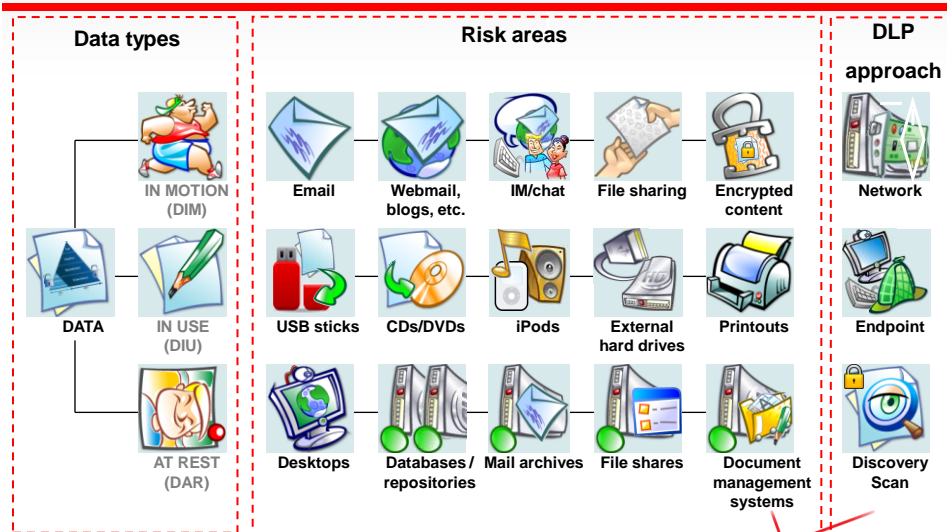
Challenges in data protection technologies and systems



Stefano Ciminelli
 Team Leader, EMEA Business Optimisation & Resilience

October 06th, 2011

Define Data Protection Data Types, Risk Areas, and Approaches



Source: Forrester Research

Who should protect what? Industries Most Concerned

	Privacy regulations	Governance & liability	IP & confidential	Consumer pressures
Financial services	●	●	●	●
Retail	●	●	●	●
Entertainment	●		●	
High-tech			●	
Healthcare & insurance	●			●
Manufacturing			●	
Pharmaceuticals	●	●	●	
Energy		●	●	
Government	●	●	●	●

Source: Forrester Research



3

Data protection Challenges



The daydreams of cat herders...



4

Challenges

Misconceptions

- **‘Act first then think’**
 - A lot of DLP projects start without a clear goal
 - Lack of a clear data protection policy
 - Lack of internal awareness around data protection
- **‘Hey Dude, run a pilot first...’**
 - Pilots are beneficial to create awareness (but not *really* for real...)
 - Deploying DLP technologies requires
 - clear vision
 - resources
 - Skills
- **‘Sniff the network, add boxes and that’s it...’**
 - Network security = IT knows what is right or wrong
 - Data security = only the business (data owners) really understands the value of the information



5

Data leakage

Typical scenario – “inside job”

Profile of the “leaker”

- Willing internal people, like:
 - Disloyal employee
 - Untrustworthy third-party contractor
- Unwilling internal people, like:
 - Sysadmin or application power-user accidentally leaking sensitive data

Timeframe

- Can go unnoticed for years
 - Log files can be tempered, destroyed, replaced...
 - Based on human trust and natural social engineering



6

Data leakage response

Some real case-studies

Leakage methods	Some possible countermeasures
<p>Data leaked to the "cloud"</p> <p>Data uploaded to malicious web-sites</p>	<ul style="list-style-type: none"> - Encrypt sensitive data (and do a proper key-management) - Network DLP solution can monitor and alert on-line if sensitive data are travelling on the network - Endpoint DLP to detect misuse of sensitive data on a desktop / laptop (copied in RAM, stored in temp folders, ...)
<p>Sensitive data printed and physically carried out of the company</p>	<ul style="list-style-type: none"> - ERM (<i>not 100% mature yet</i>)
<p>Sensitive data copied on removable medias (USB sticks, external hard drives, iPods ...)</p> <p>Loss or steal of a mobile device (Blackberry, iPhone ...) containing sensitive data</p>	<ul style="list-style-type: none"> - Endpoint DLP solution can prevent having an external media mounted on the filesystem - Mobile security best-practices (i.e. encryption of mobile devices) should be implemented



7

Case study

Example from the utility industry (electric and natural gas industry)

Problem	<ul style="list-style-type: none"> - Mainly concerned with past leakages of Intellectual Property files - Distributed R&D laboratories over Europe and Middle-East
Strategy and risk evaluation	<ul style="list-style-type: none"> - Identify several "patterns" to be used as a search template - Data Discovery mission in order to find where Intellectual Properties were stored (willingly or not...) - Phased approach, a small subset of systems at a time - Review and update the data classification policy - In parallel, review user access rights to sensitive systems / data



8

Case study

Example from the utility industry (electric and natural gas industry)

Data protection
enforcement

Phase 1:

- Deployed network DLP solution at network perimeter
- Deployed a host Endpoint DLP solution (integrating different vendor!)

Phase 2:

- Implemented white-listing and traffic inspection for https and e-mail
- ERM solution deployed for Autocad drawings and PDF documents
- Firewall and routers rules audit and review

Phase 3:

- Security hardening on all IT systems hosting sensitive data
- Define, document and fully test the Disaster Recovery Plan



verizonbusiness

9

Data protection

Effective approach



"Dude...you have data leakage."

Source www.adexchanger.com

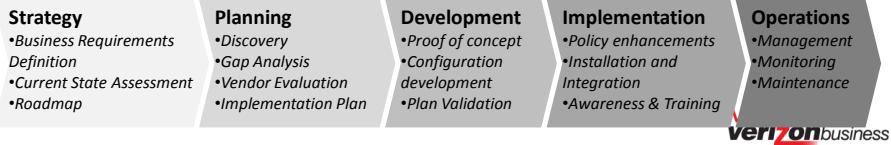
10

verizonbusiness

DLP Approach Overall Strategy

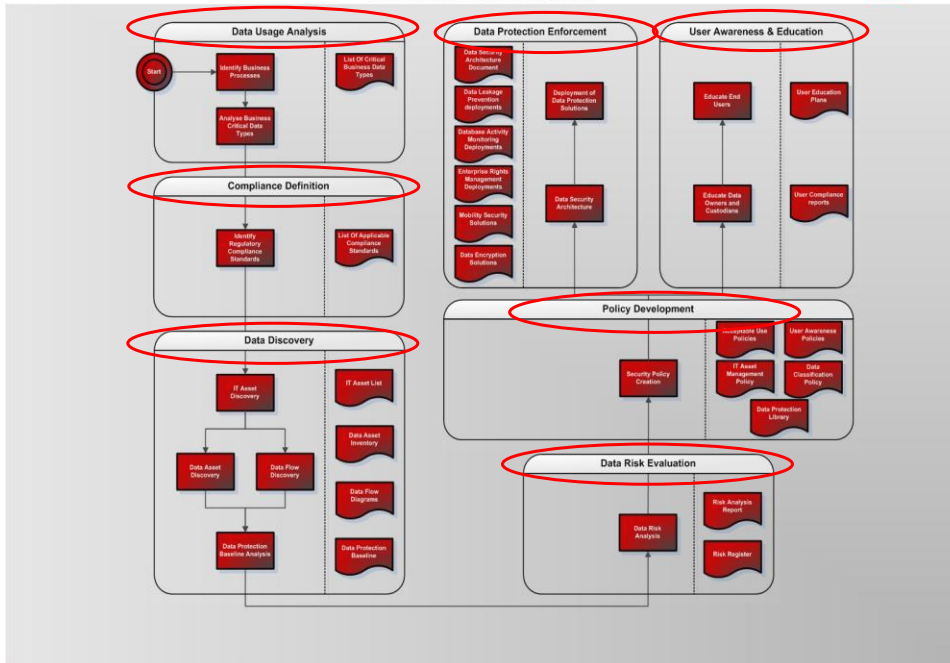
Our proposed strategy for DLP axes on 3 pillars:

- **What** data is critical to my business?
- **Where** is my critical data?
- **How** can I protect my critical data?



11

Verizon Business Data Protection Framework



Questions?

