SECURITY SUMMIT

Le quattro dimensioni di un progetto DLLP di successo

Oracle Community For Security

Atelier Tecnologico - 16 marzo 2011
Andrea Zapparoli Manzoni / Paolo Capozucca

GRUPPO TERASYSTEMI

Success rate dei progetti DLLP ?

GRUPPO TERASYSTEMI

Project Category	Project Description	2000 Results	2009 Results
Project Success	The project is completed on-time and on-budget, with all features and functions as initially specified	16.2%	32%
Project Challenged	The project is completed and operational but over-budget, over the time estimate, and offers fewer features and functions than originally specified	52.7%	44%
Project Impaired	The project is cancelled at some point during the development cycle	31.1%	24%

La Governance dei progetti IT sta migliorando, ma il tasso di successo è ancora al 32%.

I progetti DLLP, per la loro novità, sono potenzialmente soggetti ad un tasso di failure maggiore.

Tabella 1: Standish CHAOS Survey 2010

Le cause sono molteplici

GRUPPO TERASYSTEM

Principali cause di fallimento / complicazioni nei progetti IT[1]

- **Insufficient board-level support**
- **Unrealistic expectations of the organizational capacity and capability**
- **Over-estimation of benefits / under-estimation of total costs**
- **The organization fails to change its culture**
- **Insufficient engagement of stakeholders**

Non è possibile limitarsi ad implementare una soluzione tecnologica nella speranza che la sola applicazione degli strumenti di mercato possa risolvere ogni problema…

1: Standish CHAOS Survey 2010

Un esempio recente…

or somehow obtained it, the cost to the state would be significant.	individuals, businesses, the economy, and to governments is substantial.
3. Budget. The requested budget to implement a DLP solution designed to monitor and mitigate loss of sensitive data over the Internet is $530K	A. Overall budget, subtotaled for each cost category for each fiscal year of the project: a. Hardware: (with software) $400K (One time) $50K (Ongoing) b. Software: See above c. Contracted Services: $80K d. FTP's: N/A e. Training: N/A B. Request is for General Funds, other sources will be considered over time. C. Constraints are considerable in this economic environment. General Funds are not likely to be available. D. One contracted security analyst will be required to manage the system and the agency responses.

Progetto per sistema di DLLP del Governo dell'Idaho, 2010

Cosa c'è che non va?

Tabella 2: Idaho ITRMC DLP Project Summary 2010 - Budget

Un esempio recente…

GRUPPO TERASYSTEMI

Chart C **Cost Benefit Chart**

Approximate 1% of Idaho population	Cost for notification each individual record	Cost of notification	Potential suits for damages	Cost of full DLP solution - network & data at rest	Less robust DLP solution - network
150,000	$230	$34,500,000	uncertain	$680,000	$530,000
			Potential Savings:	$ 33,120,000	$ 33,970,000

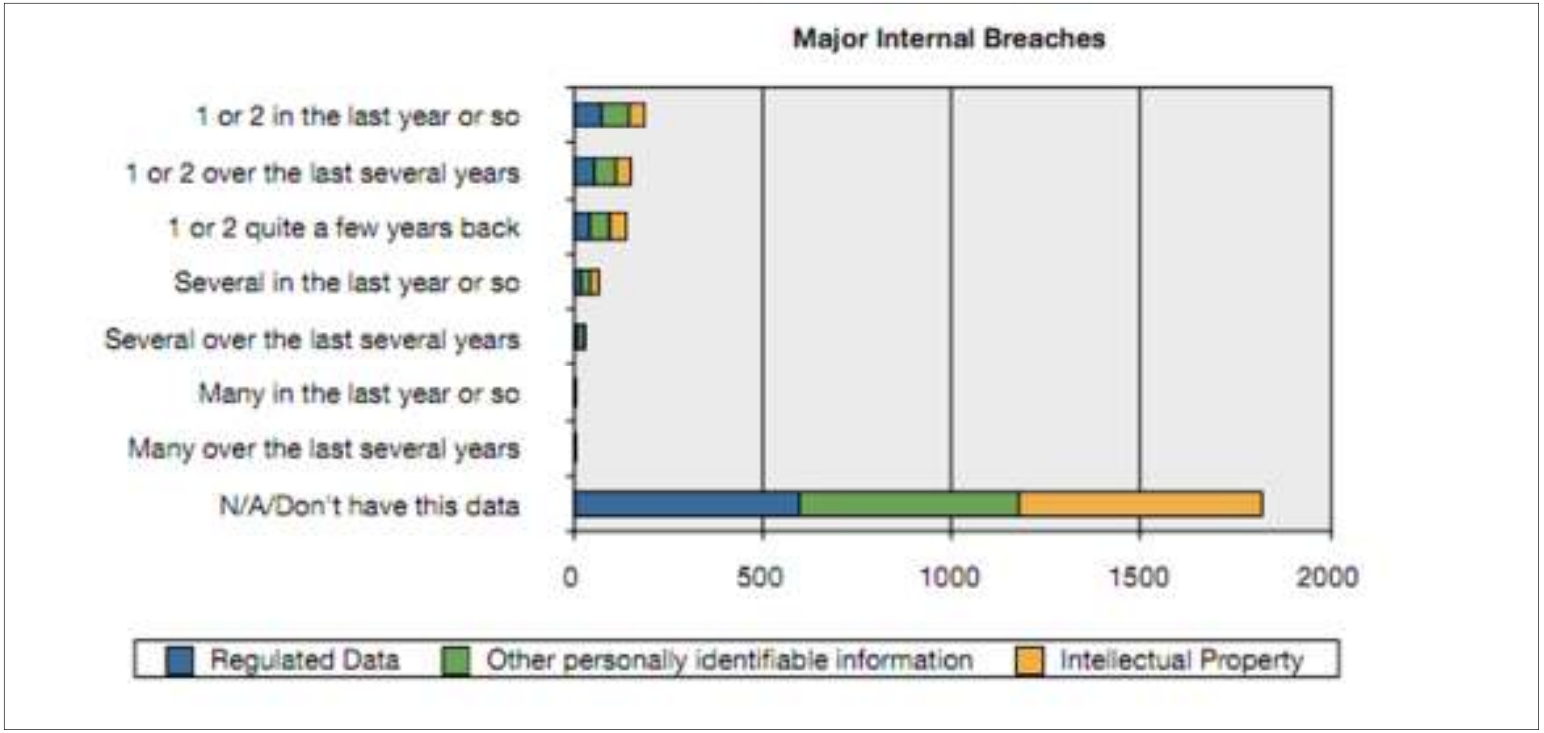
Come NON impostare un progetto DLLP:

- **Semplificare il rapporto costi / benefici**
- **Non considerare tutte le dimensioni non tecnologiche del progetto**
- **Non considerare tutte le problematiche trasversali al progetto**

E gli errori si pagano!

Tabella 3: Idaho ITRMC DLP Project Summary 2010 – Chart C

Si OK, ma il DLLP è *strategico*!



...Wikileaks docet….

Tabella 4: Securosis Data Security Survey 2010 - Awareness

Allora facciamolo come si deve

GRUPPO TERASYSTEM

Il DLLP non è un problema (solo) dell'IT.

Per avere le migliori probabilità di successo un progetto DLLP in ambiente Enterprise deve essere impostato, sviluppato e gestito nel tempo lungo quattro dimensioni:

- **il piano organizzativo**
- **quello gestionale-formativo**
- **quello amministrativo-legale e**
- **quello tecnologico.**

tenendo conto di una serie di componenti sistemiche e della necessità di una robusta impostazione di ICT Security alla base di tutto.

Gli elementi sistemici

GRUPPO TERASYSTEM

Esistono inoltre una serie di componenti "sistemici" che sono trasversali a tutti i piani e che vanno accuratamente inseriti nel disegno complessivo del progetto.

Ricordiamo i principali:

- **l'ingegneria dei ruoli**
- **l'identity management**
- **l'access management e l'autenticazione**
- **la classificazione delle informazioni**
- **il digital asset management**
- **il monitoraggio non ripudiabile**

…vi ricorda qualcosa?

Il piano organizzativo

GRUPPO TERASYSTEMIT

All'interno della dimensione organizzativa vengono definite:

- **le policy**
- **le linee guida**
- **i workflow**
- **le responsabilità**
- **le metodologie di auditing e di controllo del sistema**
- **il processo di assessment continuo dell'efficacia della soluzione**

E' estremamente importante che siano coinvolti in modo stabile ed attivo tutti gli attori interessati, dal top management al HR al Legal all'IT alla Security ai collaboratori, e che sia istituito un comitato multidisciplinare di supervisione e controllo dei KSI.

Il piano gestionale e formativo

GRUPPO TERASYSTEM

La dimensione gestionale include tutte le attività necessarie ad implementare i vari aspetti della dimensione organizzativa in modo organico e coerente, mantenendo i processi efficienti ed agili.

Due aspetti particolarmente sottovalutati, oltre a quello gestionale, sono di particolare importanza per tutti gli attori coinvolti:

- **formazione permanente ed awareness rising**
- **comunicazione dei risultati ottenuti in forma chiara ed utilizzabile**

….in fondo il DLLP è una gran scocciatura ☺

Il piano legale-amministrativo

GRUPPO TERASYSTEM

La dimensione amministrativa-legale include tutti i processi necessari a far evolvere il sistema DLLP nel rispetto delle normative, delle policy stabilite e dei livelli di rischio accettati.

Un sistema DLLP non è del tipo "fire and forget", va continuamente adeguato, possibilmente anticipando le problematiche, perché:

- **Le normative cambiano**
- **Le tipologie di informazioni trattate cambiano**
- **Le tecnologie cambiano più velocemente delle norme e delle policy**
- **Le minacce si evolvono più rapidamente delle tecnologie**

Questi processi di mantenimento della compliance nel tempo sono fondamentali per il successo di un sistema DLLP, e spesso sono sottovalutati in fase di progetto.

Il piano tecnologico

GRUPPO TERASYSTEMIT

La dimensione tecnologica comprende tutte le attività di disegno, implementazione, roll-out, verifica e manutenzione del sistema in esercizio.

Oggi esistono ottime soluzioni di mercato, ma il problema è:

- Integrarle con le altre piattaforme e funzioni coinvolte
- Mantenerle aggiornate, reattive ed efficienti
- Essere in grado di farle scalare in vista di nuovi oneri / esigenze
- Mantenere i costi allineati con i budget e con il ROSI previsto

Soprattutto, il problema è usare efficacemente le suite esistenti, dal momento che spesso si finisce per attivare ed utilizzare il 50% delle features presenti.

Il tempo è tiranno….

GRUPPO TERASYSTEM

GRAZIE!