[cyber|mobile|cloud] Security (& privacy), by design!

LucaBechelli
ICT Security Consultant
Socio Clusit Associazione Italiana per la Sicurezza Informatica
Direttivo e Comitato Tecnico Scientifico
www.bechelli.net luca@bechelli.net

L'importanza dell'informazione

Una informazione non è mai solo "significato". Nell'azienda, può essere (almeno):

L’importanza dell’informazione

L’informazione è pertanto “amorfa”, ed estremamente pervasiva nell’azienda

L’importanza dell’informazione

E’ l’unico asset (oltre alle persone!) in grado di mettere in relazione le altre tipologie di asset tra loro, dandone valore e identità

Valore e Identità

Veni Vidi Vici

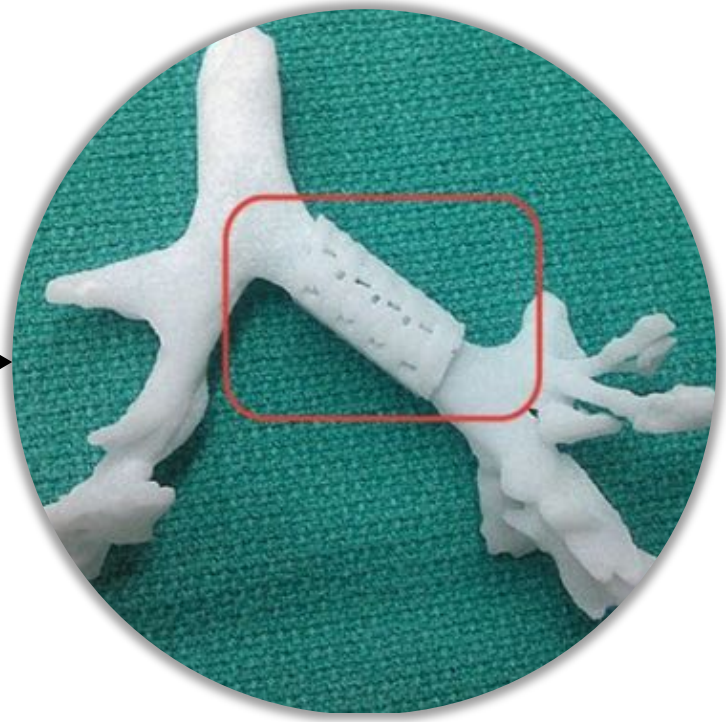
L'importanza dell'informazione

Più spesso di quanto sembrerebbe, le organizzazioni tendono a sottovalutare la dipendenza che hanno non tanto dalle informazioni, ma dagli strumenti mediante i quali queste sono accessibili ed utilizzabili

L'importanza dell'informazione

del controllo

?



Security by Design

Security by Design

Cosa è:

NON

> *Without Security by Design we have Security by Afterthought.*
>
> *Security by Design at the product level is a beginning not an end.*
>
> *But it is an essential beginning to building secure and resilient systems and networks and to delivering secure and reliable services over them.*

(www.eurim.co.uk)

HACKINBO

Security by Design

Cosa è:

DESIGNED

> As IT becomes more of a utility, users are going to buy a whole lot more services than products. And by nature, services are more about results than technologies. Service customers -- whether home users or multinational corporations -- care less and less about the specifics of security technologies, and increasingly expect their IT to be integrally secure.
>
> (Bruce Schneier)

from the

GROUND

up to be

SECURE

Security by Design

Cosa è:

Include la **gestione**, gli **obiettivi**, i **requisiti**, il **budget**, le **competenze**, la **metodologia**, i **controlli**, gli **strumenti**, ...

Integrazione della **Sicurezza** in tutto il **ciclo di vita** del progetto

Security by Design

Cosa fare:

"*Security activities should be physically and logically integrated into the SDLC policy and guidelines*

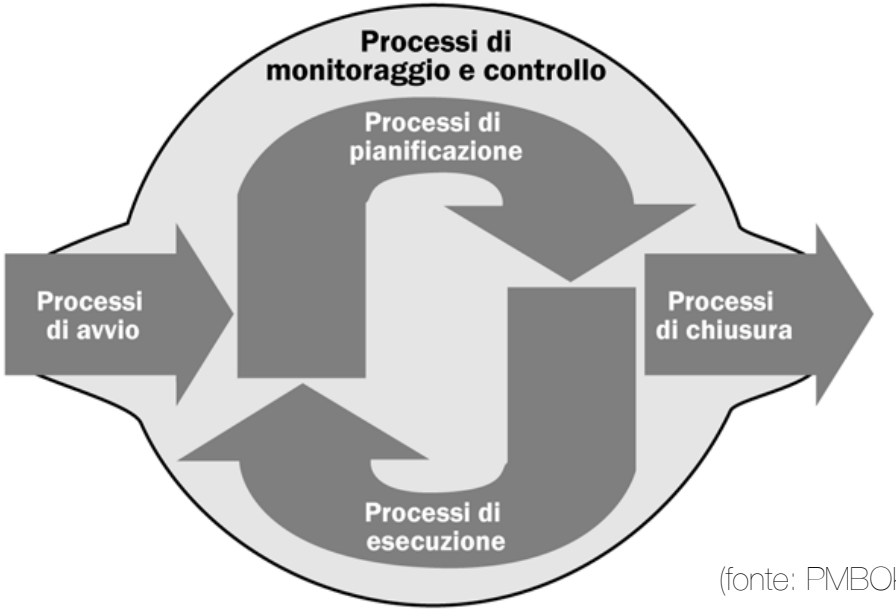
versus maintaining them in a separate, complementary document or security life cycle."

(NIST Special Publication 800-64)

"*This ensures a wider audience and decreases the need for the reader to reference multiple documents unnecessarily. Of course, security integration can and should reference supplemental process documents that provide further details*"

Cosa fare:

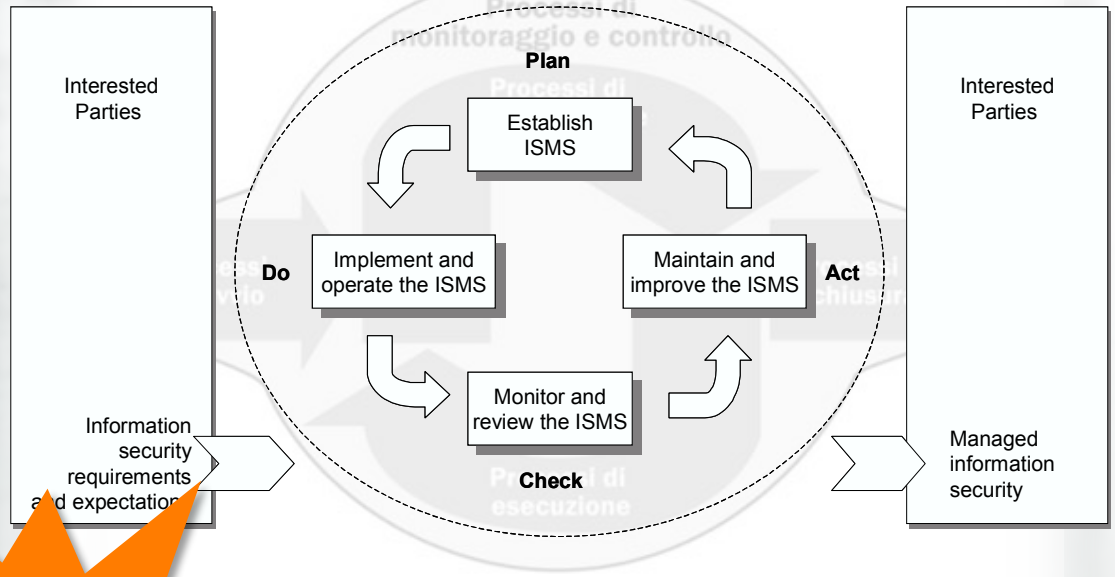
Il carattere integrativo del Project Management …



(fonte: PMBOK)

Cosa fare:

Il carattere integrativo del Project Management …



Good News!

…ed il processo di sicurezza!

(fonte: ISO/IEC 27001)

..se la felicità è il viaggio e non la meta...
(Crystal Boyd)

Cosa fare:

Security by Afterthought.

Ad oggi, nella maggior parte delle aziende, l'attuazione delle misure di sicurezza si concentra in questa fase

Figure 1: Relative Costs to Fix Software Defects (Source: IBM Systems Sciences Institute)

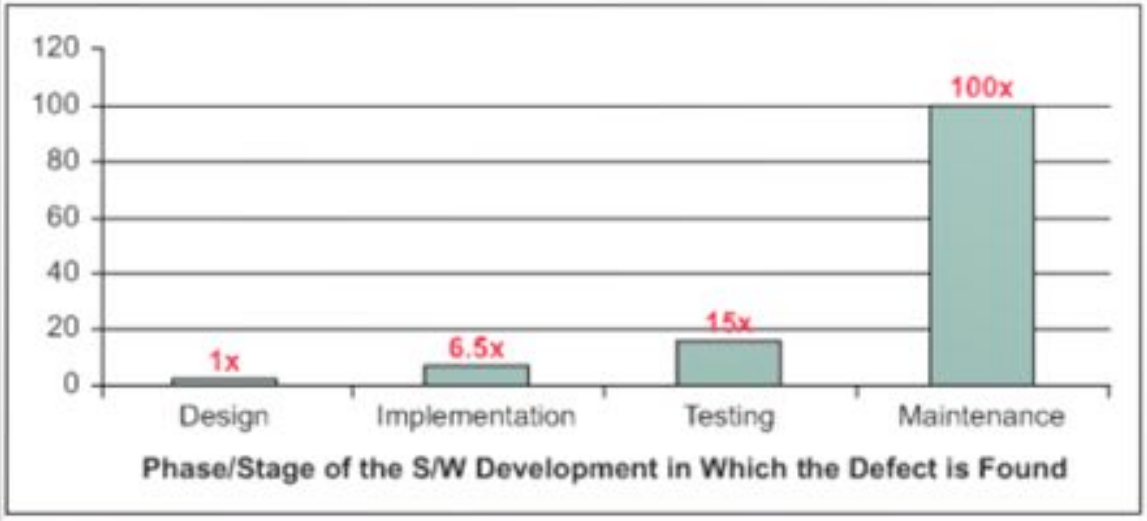
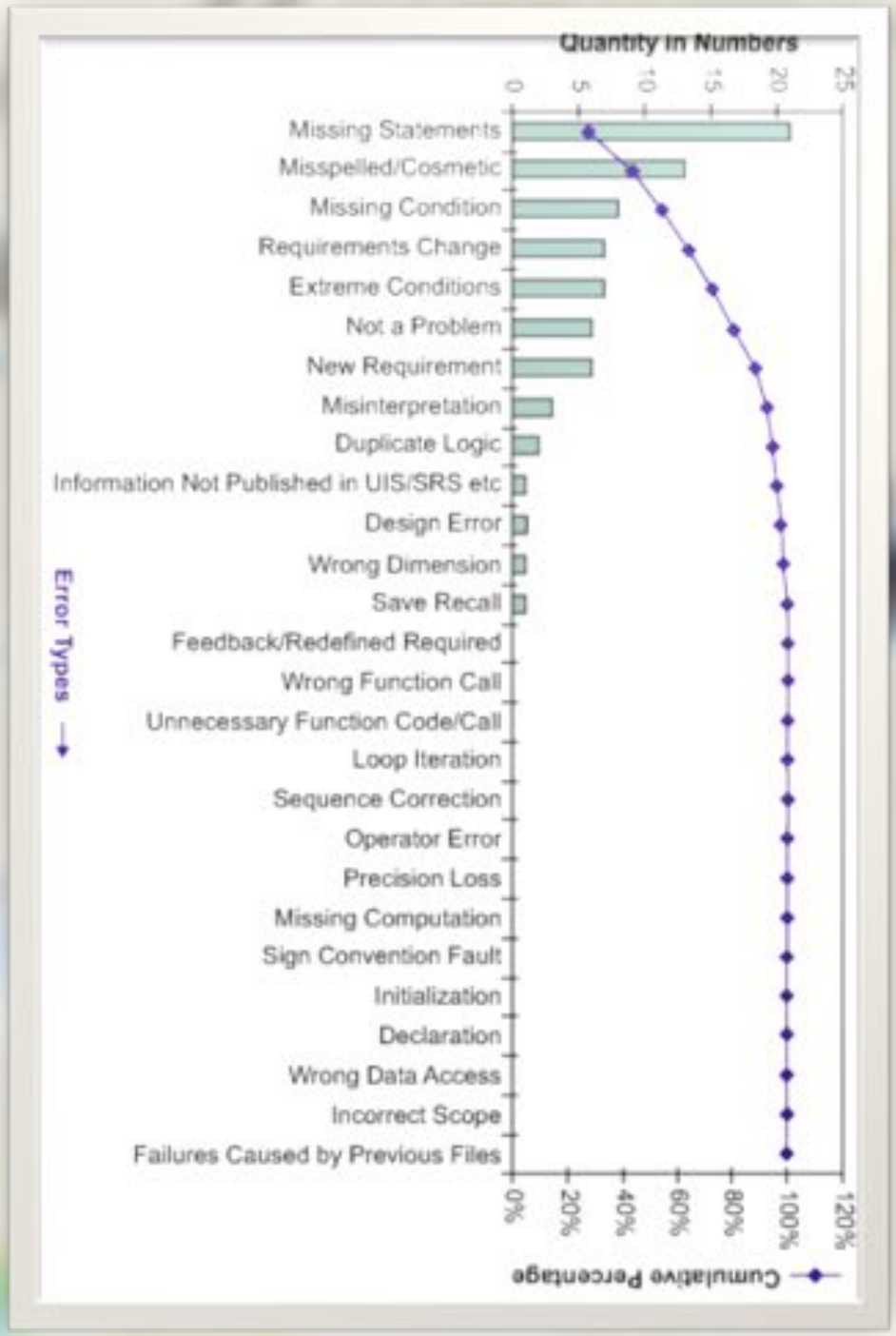


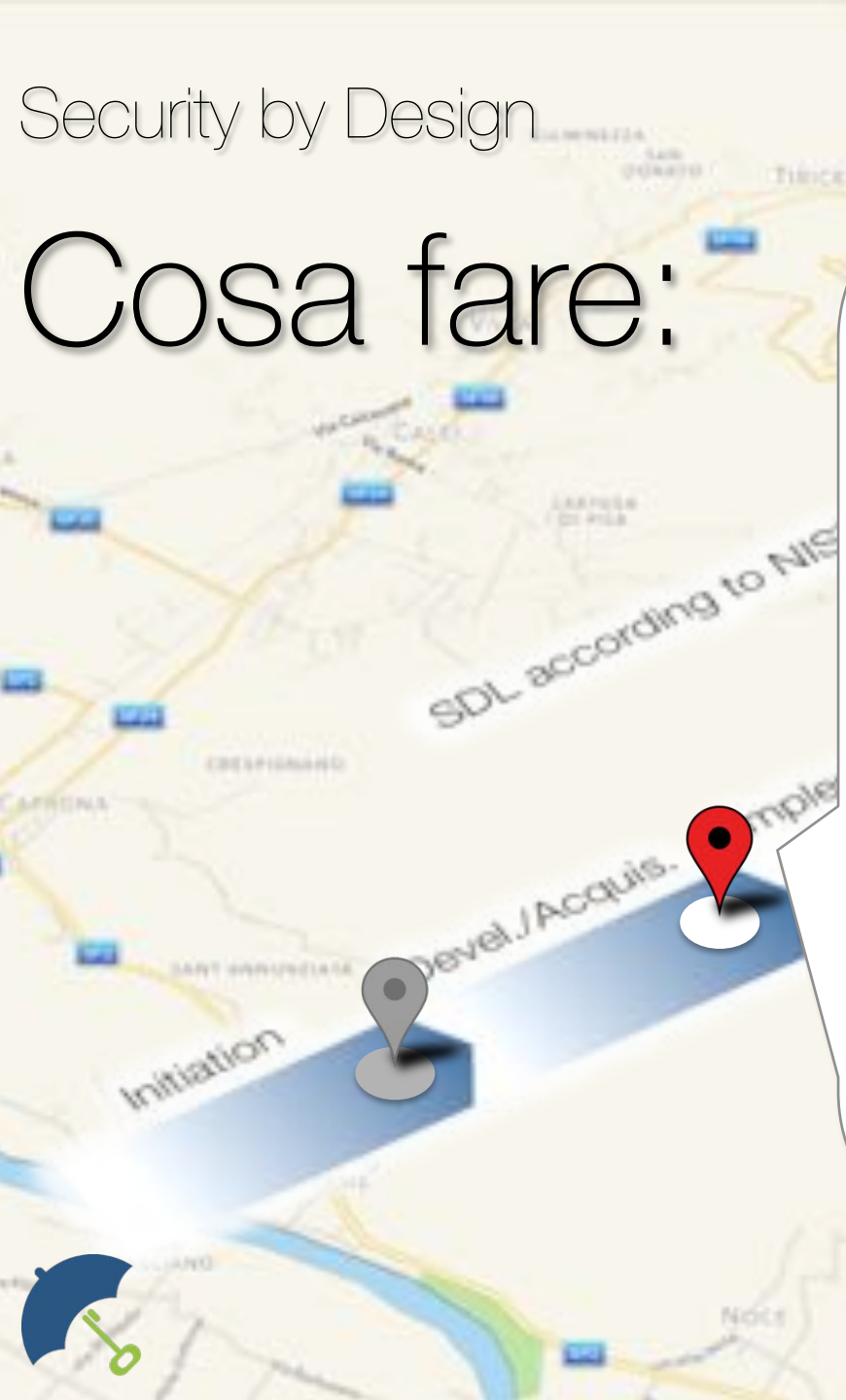
Figure 3: Origin of Software Defects (Source: Crosstalk, the Journal of Defense Software Engineering)


Quantity in Numbers
0
5
10
15
20
25
Missing Statements
Misspelled/Cosmetic
Missing Condition
Requirements Change
Extreme Conditions
Not a Problem
New Requirement
Misinterpretation
Duplicate Logic
Information Not Published in UIS/SRS etc
Design Error
Wrong Dimension
Save Recall
Feedback/Redefined Required
Wrong Function Call
Unnecessary Function Code/Call
Loop Iteration
Sequence Correction
Operator Error
Precision Loss
Missing Computation
Sign Convention Fault
Initialization
Declaration
Wrong Data Access
Incorrect Scope
Failures Caused by Previous Files
Error Types
0%
20%
40%
60%
80%
100%
120%
Cumulative Percentage

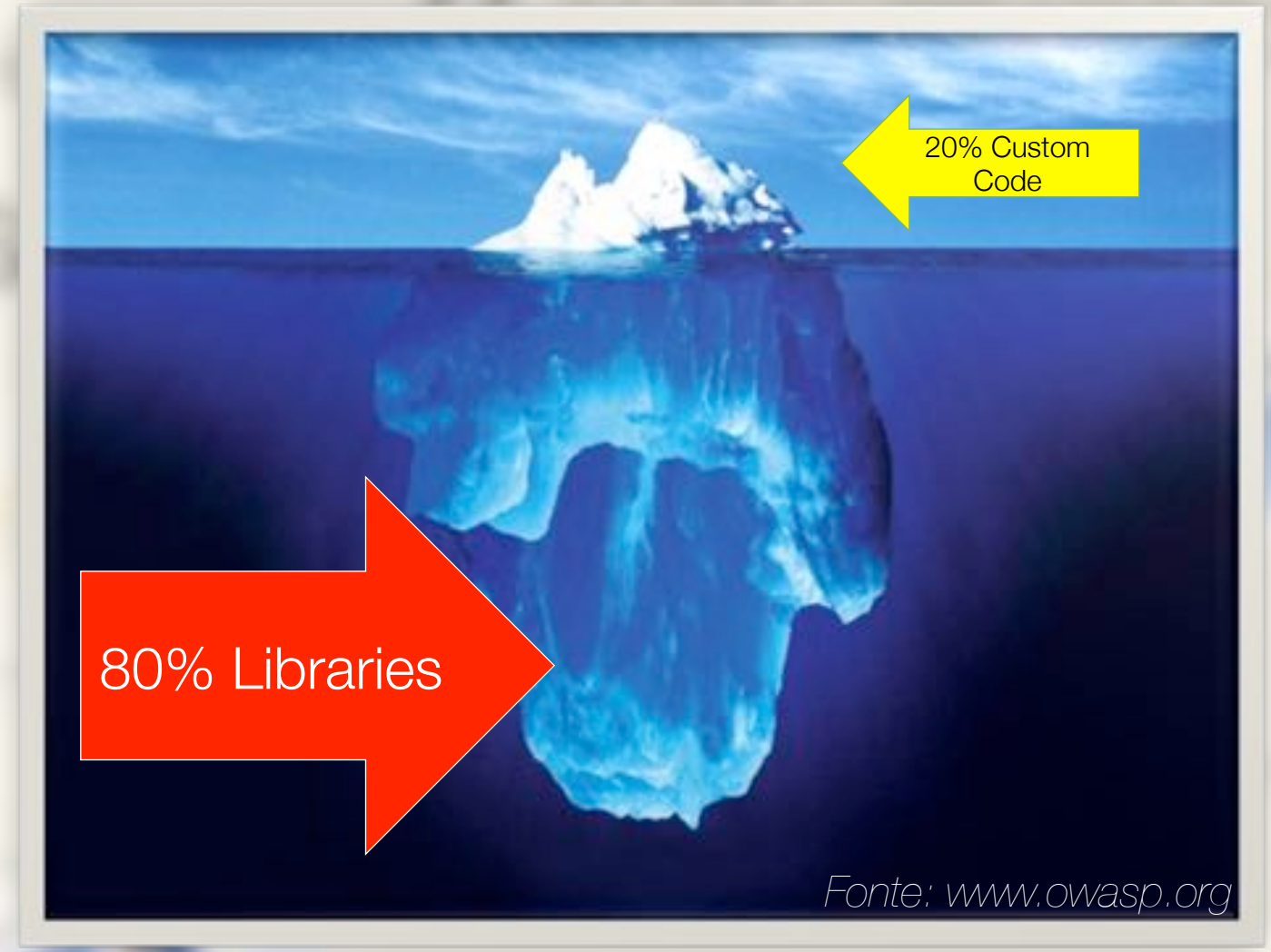
Cosa fare:

- Nell'ambito della raccolta dei requisiti, prevedere anche i requisiti di sicurezza:
  - Basati su esigenze (anche implicite) degli stakeholder
    - Interni: aziendali, di product management, …
    - Esterni: contesto di utilizzo, clienti, competitor, …
  - Personalizzati sulla base del contesto
  - Derivanti da minacce note e serie storiche;
  - Basati su standard internazionali
  - Derivanti da normative vigenti e "prevedibili"
  - Determinati a partire da risk assessment, ma sopratutto di "common sense"
- Il budget del progetto deve prevedere una voce per la sicurezza, anche e sopratutto per bilanciare tali costi rispetto all'impegno complessivo da sostenere

Cosa fare:



- Applicare principi di sicurezza nel design. Es:
  - Basati su best practices e standard internazionali di sicurezza
  - Derivati da specifiche di sicurezza di prodotto / tecnologia
    - Esempi: Least Privilege, Defense in depth, Need-to-Know, Updatability, Accountability
- Identificare i principali rischi afferenti la soluzione da realizzare, e definire le relative contromisure. Es:
  - Spesso i rischi si nascondono in assunzioni/prerequisiti
  - Non fidarsi solo nella “riduzione della superficie di attacco”
  - Stabilire un modello di minacce
- Scegliere le tecnologie da utilizzare (anche) sulla base di criteri di sicurezza
  - N.B.: utilizzando protocolli e tecnologie standard (internazionali o di mercato)
  - Scegliere tecnologie e soluzioni “sostenibili” per la successiva operation/maintenance



The security design principles apply to the product and to all product components, not only to components with identified security functionality

(Security by Design with CMMI for Development)

Security by Design

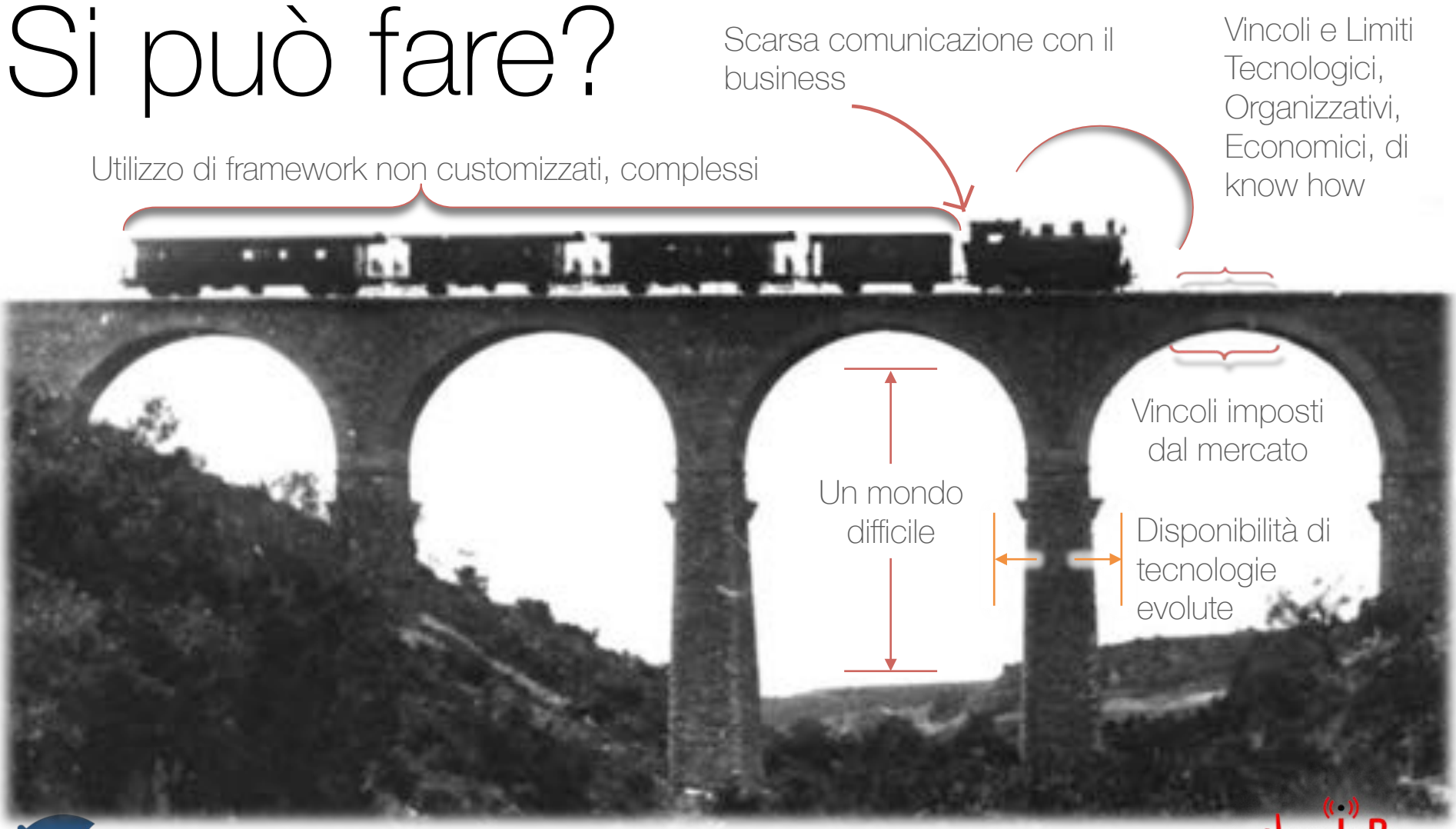
Cosa fare:

- Integrare i controlli di sicurezza nell'ambito in fase di test. Es:
  - Dallo unit test ai test specifici di sicurezza, come Vulnerability Assessment / Penetration Test e secure Code Review
  - Considerare l'attuazione di test di sicurezza indipendenti da parte di terze parti

- Fare riferimento ad aspetti di sicurezza nell'ambito dell'implementazione. Es:
  - scegliere linguaggi, API, parametri di configurazione dei compilatori che assicurano maggiore correttezza e robustezza nel codice…
- Adottare strumenti di Software Quality Mgmt.
- Utilizzare strumenti di secure code review in fase di sviluppo
- Implementare meccanismi di supporto all'aggiornamento di tutte le componenti

- Documentare le funzionalità e gli aspetti di sicurezza del progetto. Es:
  - Caratteristiche di sicurezza attese dell'ambiente di esecuzione
  - Descrivere gli aspetti che possono avere impatti nella gestione sicura della soluzine: protocolli, porte utilizzate, regole di gestione di password e account, …
  - Misure e accorgimenti per la configurazione sicura
  - Errori e messaggi di warning
  - Informazioni di log

Si può fare?


Scarsa comunicazione con il business
Vincoli e Limiti Tecnologici, Organizzativi, Economici, di know how
Utilizzo di framework non customizzati, complessi
Vincoli imposti dal mercato
Un mondo difficile
Disponibilità di tecnologie evolute

Security by Design

Come farlo:

The organization … requires appropriate processes that integrate these techniques and capabilities for a sustainable effort to develop secure products beyond trial-and- error

(Security by Design with CMMI for Development)

Security by Design

Come farlo:

L'importanza degli standard;

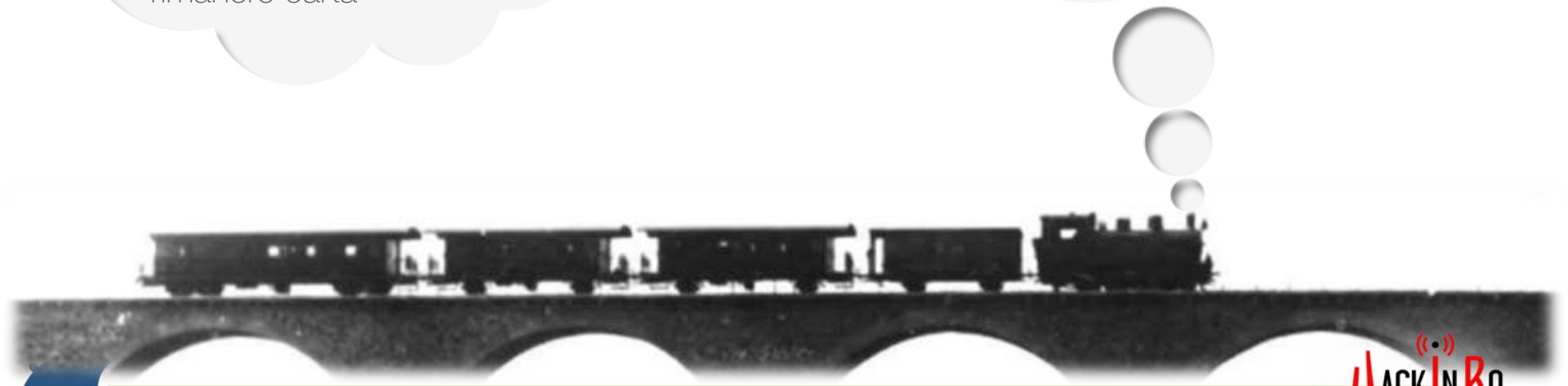
Come farlo:

Passare da “object reuse” a “ICT reuse”

- L’azienda:
  - ha un A.D., un LDAP, una piattaforma IAM?
  - L’azienda utilizza un SIEM / Log Collector?
  - Quanto cambieranno mai le normative?
- Le metodologie, i tool, gli standard non possono essere adottati come una iniziativa del singolo progetto

Investire sulle persone:

- Le tecniche di secure coding, la sicurezza nella maintenance e le buone pratiche non devono rimanere carta



1999 - 2015


Google!
BETA
Search the web using Google
Google Search
I'm feeling lucky
More Google!
Copyright ©1999 Google Inc.


Microsoft
Microsoft
Windows98
Upgrade


U.S. Robotics
56K Message Modem


Microsoft
Windows95

Privacy “by design”

“…la garanzia della privacy deve costituire idealmente un modo di operare di default di un’organizzazione.”

1. **Proattivo** non reattivo; **prevenire** non correggere
2. Privacy come impostazione di **default** (*…se un individuo non fa nulla, la sua privacy rimane ancora intatta. Non è richiesta alcuna azione da parte dell’individuo per proteggere la propria privacy…*)
3. Privacy incorporata nella **progettazione**
4. Massima **funzionalità** – Valore positivo, non valore zero
5. Sicurezza fino alla **fine** – Piena protezione del ciclo vitale
6. Visibilità e trasparenza – Mantenere la trasparenza
7. Rispetto per la privacy dell’utente – **Centralità dell’utente**

(domande?)

GRAZIE!