

Università di Venezia

Corso di Laurea in Informatica

“Laboratorio di Informatica Applicata – Introduzione all’IT Governance”

Lezione 10 e 11



Marco Fusaro – KPMG S.p.A.

Risk Analysis

I termini “risk analysis” e “risk management” sono di per sé generici → devono essere corredati da qualche attributo che ne specifichi l’ambito.

Le tecniche di risk analysis assumono forme diverse secondo l’ambito cui si applicano:

- Project Risk Management
- IT Security Risk Analysis
- IT Risk Management
- ...

Per l’IT è di particolare importanza una classe di rischi associata all’informazione e al processo che la genera e la tratta → IT Security Risk Analysis.

IT Security Risk Analysis

Due possibili approcci:

➤ Approccio “qualitativo”

- ✓ E’ quello che vedremo nelle prossime slide.
- ✓ Fornisce valutazioni in termini di criticità dei dati per il business aziendale.

➤ Approccio “quantitativo”

- ✓ Fornisce valutazioni in termini monetari
- ✓ Brevi accenni al termine della lezione

IT Security Risk Analysis

L'IT Security Risk Analysis procede dall'assunzione che il bene più importante a livello di Sistemi Informativi in un'azienda è l'informazione.

E' importante, quindi, garantire la **sicurezza** del patrimonio informativo aziendale.

Cosa significa **sicurezza delle informazioni?**

?

IT Security Risk Analysis

La criticità dell'informazione per il business aziendale si può misurare in termini di:

- C Confidentiality (Riservatezza)
Accessibilità permessa solo a chi è autorizzato
- I Integrity (Integrità)
Accuratezza e completezza
- A Availability (Disponibilità)
Possibilità di accesso quando richiesto

Proporzionalità tra il valore dell'informazione e la criticità

IT Security Risk Analysis

Esempi

I dati riguardanti i movimenti di conto corrente del cliente di una banca:

- Confidenzialità **Alta**
- Integrità **Alta**
- Disponibilità **Alta**

IT Security Risk Analysis

Esempi

Le quotazioni di borsa proposte da un sito di trading alla propria clientela:

- Confidenzialità **Bassa**
- Integrità **Alta**
- Disponibilità **Alta**

IT Security Risk Analysis

Esempi

I dati relativi ai fabbisogni di materia prima per un'azienda di produzione:

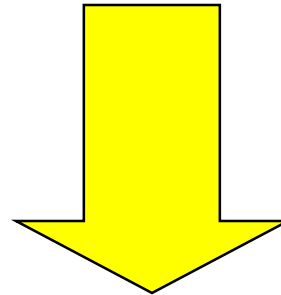
- Confidenzialità **Bassa**
- Integrità *Dipende*
- Disponibilità *Dipende*

Dipende dal costo del materiale che si acquista, dalla politica di riordino, ...

IT Security Risk Analysis

Dipende

Il “dipende” implica che la criticità delle informazioni per i processi aziendali non può essere definita a priori, ma deve essere valutata con chi all’interno dell’azienda usa o conosce il valore associato all’uso del dato.



Non è la funzione IT a dover definire la criticità delle informazioni, ma sono le altre funzioni aziendali a doverlo fare.

IT Security Risk Analysis

L'informazione ha un "valore"; questo valore può essere posto, in modo più o meno diretto, in relazione ad un corrispondente valore economico.

L'**IT Security Risk Analysis** si pone come obiettivo la valutazione del grado di sicurezza delle informazioni.

Dobbiamo "**misurare**" il livello di sicurezza del patrimonio informativo → **serve un modello!**

Nelle prossime slide:

- verrà presentato un modello *molto* semplificato per la misurazione della sicurezza delle informazioni
- verranno mostrati i passi necessari per lo svolgimento di un'attività di IT Security Risk Analysis

IT Security Risk Analysis

Un modello (1)

Le informazioni aziendali sono custodite nei sistemi informatici aziendali (host, personal computer, ecc.).

La sicurezza delle informazioni è messa a repentaglio da minacce che sfruttano vulnerabilità.

Minaccia entità che può causare danno

Vulnerabilità condizione di debolezza che una minaccia può sfruttare per manifestarsi

Suscettibilità = f (minaccia, vulnerabilità)

Suscettibilità potenzialità della minaccia dovuta alla combinazione con la vulnerabilità

IT Security Risk Analysis

Un modello (2)

Il valore delle informazioni è proporzionale alla loro criticità misurata in termini di confidenzialità, integrità e disponibilità.

$$\text{Valore} = f (C, I, A)$$

Il rischio è funzione della probabilità dell'evento (susceptibilità) e dell'impatto (valore delle informazioni)

$$\text{Rischio} = f (\text{susceptibilità}, \text{valore})$$

IT Security Risk Analysis

Esempi di classificazione delle Minacce

Interne / esterne	(hacker / dipendente)
Sofisticate / non sofisticate	(preparato / dilettante)
Ostili / non ostili	(intenzionale / per errore)
Ambientali / umane	(incendio / persona)

Esempi di Minacce:

- un dipendente che introduca intenzionalmente o meno un “errore” in una procedura informatica
- il cliente di una banca on-line che acceda per errore ai movimenti di conto corrente di un altro cliente
- un dipendente che cancelli per errore un file importante dal file server

IT Security Risk Analysis

Esempi di classificazione delle vulnerabilità

N.B. nella tabella sono presentati a titolo esemplificativo “controlli” → si assume che la loro mancanza costituisca una vulnerabilità

Classificazione	Tecnica	Organizzativa
Identificazione e autenticazione	Meccanismi di logon Meccanismi per la sostituzione autonoma della password	Procedura per la distribuzione sicura di profilo e password
Controllo accessi	Blocco delle password dopo N tentativi di accesso falliti Meccanismo di scollegamento delle sessioni inattive dopo N minuti	Diritti di accesso assegnati con la politica “tutto ciò che non è permesso è proibito”
Tracciamento	Registrazione delle transazioni associate all'utente	Conservazione per N mesi dei log di tracciamento Effettuazione attività di analisi dei dati tracciati
Precisione	Presenza di un antivirus aggiornato ogni N giorni	Separazione dei ruoli tra sviluppatori del software e chi trasferisce il software in produzione
Affidabilità	Presenza di dispositivi per il backup dei dati su supporto magnetico	Conservazione off-site dei nastri di backup
Sicurezza fisica	Server conservati presso una sala macchine ad accesso controllato, con impianto antincendio	L'accesso alla sala macchine è consentito solo con apposita autorizzazione
...

IT Security Risk Analysis

Case study

Un grosso gruppo industriale si è storicamente formato mediante fusioni e acquisizioni. Il management aziendale della capo gruppo ha sempre gestito le aziende sfruttando sinergie dal punto di vista della produzione, del marketing e degli acquisti, ma lasciando notevole autonomia per quanto riguarda i Sistemi Informativi.

Alcuni problemi manifestatisi a livello di Sistemi Informativi hanno avuto ripercussioni di carattere economico.

Il management di gruppo ha, quindi, deciso di svolgere un'attività di analisi per comprendere lo stato di sicurezza delle informazioni.

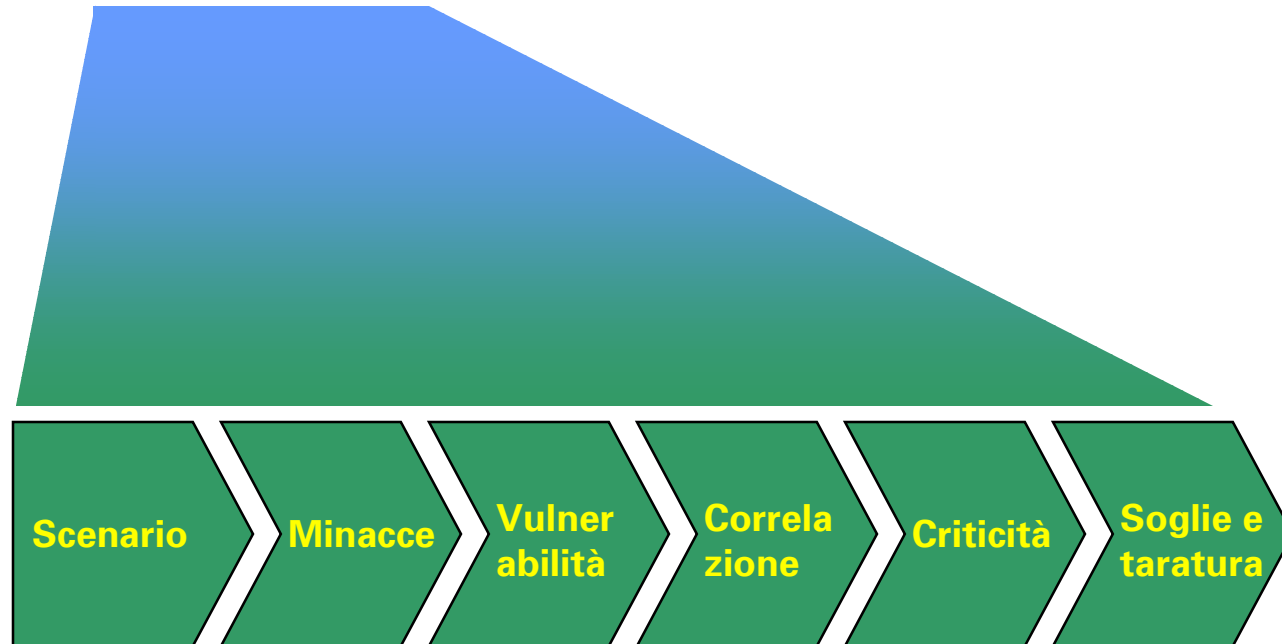
IT Security Risk Analysis



L'attività può essere svolta utilizzando un approccio di tipo IT Security Risk Analysis:

- un gruppo di studio prepara il modello e gli strumenti necessari per la raccolta delle informazioni
- le informazioni vengono raccolte mediante attività sul campo presso le varie aziende del gruppo
- viene calcolato il rischio associato ai sistemi informatici presenti nelle varie aziende del gruppo e si procede ad una presentazione al management che ha commissionato l'indagine

IT Security Risk Analysis

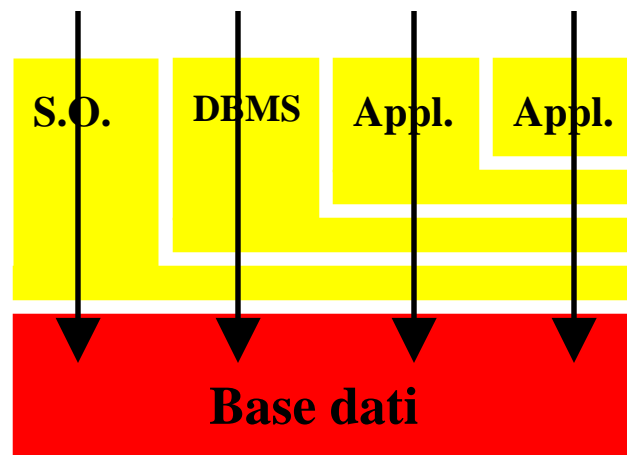


IT Security Risk Analysis

Definizione del modello e degli strumenti



Utente



Il modello prevede che ogni applicazione acceda ad una base dati logicamente e fisicamente distinta dalle altre.

Il modello prevede l'accesso alle informazioni mediante:

- il sistema operativo;
- strumenti del DBMS;
- l'applicazione proprietaria dei dati.

Le altre applicazioni accedono ai dati sfruttando funzionalità messe a disposizione dall'applicazione proprietaria dei dati.

IT Security Risk Analysis



Abbiamo introdotto alcune semplificazioni (necessarie a livello didattico, ma che rendono il modello difficilmente utilizzabile):

- ad ogni applicazione corrisponde una base dati logicamente e fisicamente distinta dalle altre;
- solo le applicazioni proprietarie dei dati accedono direttamente ai dati (in realtà trascuriamo ODBC, ecc.);
- abbiamo trascurato problematiche di rete.

Nella realtà le problematiche di rete sono fondamentali!

IT Security Risk Analysis

Classificazione delle minacce



Il modello prevede una semplice suddivisione delle minacce in:

Minacce	
Dipendenti fraudolenti	M_1
Dipendenti curiosi	M_2
Hacker competenti	M_3
Hacker non competenti	M_4
...	

Più realisticamente andrebbero combinate le classificazioni viste in precedenza.

IT Security Risk Analysis



Per la misurazione delle minacce si può utilizzare una metodologia basata sul brainstorming tra chi guida l'indagine e il management aziendale ipotizzando una scala di valori che dipende dalla granularità che si vuole ottenere nella misura.

Esempio

- 1 – minaccia poco probabile
- 2 – minaccia mediamente probabile
- 3 – minaccia altamente probabile

Una organizzazione internazionale di beneficenza probabilmente avrà poco da temere da hacker preparati ($M_3 = 1$).

Una banca probabilmente avrà timore di dipendenti fraudolenti ($M_1 = 3$).

→ È l'utente dei sistemi informativi che deve decidere!

IT Security Risk Analysis



Nota bene

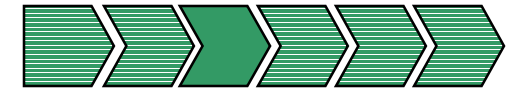
La minaccia non è, in questo modello, proporzionale al valore dell'informazione:

- il dipendente sbadato che cancella il file non è attratto dai file che contengono le informazioni più preziose
- gli incendi non sono attratti dai sistemi informatici strategici per le aziende

Un principio utilizzabile per valorizzare le minacce è considerare la storia aziendale.

IT Security Risk Analysis

Classificazione delle vulnerabilità



Il modello prevede una semplice catalogazione di vulnerabilità collegate alla mancanza di controlli minimi associati al sistema operativo, al DBMS e alle applicazioni.

Per ogni database sarà compilata, da chi conduce l'indagine, una tabella come la seguente.

Nella colonna dei valori sarà assegnato il valore 1 in caso di vulnerabilità presente e 0 in caso di assente o non applicabile.

	Vulnerabilità	V _{in}
APPLICAZIONE	Meccanismo di logon	0
	Politica di accesso "vietato tutto ciò che non è consentito"	1
	...	
SISTEMA OPERATIVO	Meccanismo di logon	0
	Scadenza della password dopo 60 giorni	0
	...	
DBMS	E' attiva una procedura per l'installazione delle patch non appena rilasciate dal produttore	1
	...	

IT Security Risk Analysis

Correlazione minacce - vulnerabilità



Le diverse vulnerabilità hanno una importanza diversa secondo le minacce.

Le correlazioni possono essere raccolte con una tabella come la seguente:

		M₁	...	M₃	...
		Dipendente fraudolento		Hacker competente	
...					
V₅	Scadenza della password	2		1	
V₆	Attività periodica di vulnerability assessment	1		2	
...					

La matrice di correlazione viene compilata dal personale che definisce il modello.

IT Security Risk Analysis

Criticità delle informazioni



L'attività di valutazione della criticità delle informazioni non può essere in carico a personale tecnico, ma deve essere in carico a personale "utente" dei Sistemi Informativi, che conosce il valore da attribuire alla riservatezza, integrità e disponibilità delle singole basi di dati.

I valori da utilizzare nell'indagine devono essere raccolti con questionari che permettano di trasformare l'esigenza di business in una esigenza tecnica.

I questionari devono essere elaborati dopo una analisi dei processi aziendali.

Si compila un questionario per ogni base dati.

IT Security Risk Analysis



Esempio:

nell'ipotesi di definire 3 valori:

1 – criticità bassa

2 – criticità media

3 – criticità alta

Criticità	Scenario per criticità bassa	Scenario per criticità media	Scenario per criticità alta	Punteggio
CONFIDENTIALITY	La divulgazione delle informazioni non comporterebbe alcun impatto	La divulgazione delle informazioni comporterebbe problemi interni all'azienda	La divulgazione delle informazioni comporterebbe problemi con entità esterne all'azienda	
CONFIDENTIALITY	
...				
AVAILABILITY	L'azienda può lavorare per alcuni giorni senza utilizzare la base dati	L'azienda può lavorare per alcune ore in caso di non disponibilità della base dati	L'azienda è bloccata in caso di non disponibilità della base dati	
...				

IT Security Risk Analysis



Come sono collegate le informazioni rilevate?

Ricordiamoci che obiettivo del lavoro è la misurazione del rischio per le informazioni. Per ogni base dati possiamo definire:

$$\underline{R}_n = (R_{Cn}, R_{In}, R_{An})$$

dove \underline{R}_n Rischio per la sicurezza della base dati

R_{Cn} Componente del rischio dovuta alla Confidenzialità

R_{In} Componente del rischio dovuta alla Integrità

R_{An} Componente del rischio dovuta alla Disponibilità

$$\underline{V}_n = (V_{1n}, V_{2n}, \dots, V_{vn})$$

dove V_{in} rappresenta le vulnerabilità rilevate per la base dati n-esima

IT Security Risk Analysis



Le minacce sono considerate in assoluto, quindi non in relazione alla base dati

$\underline{M} = (M_1 , M_2 , \dots , M_m)$ Valori delle minacce

$\underline{VAL}_n = (VAL_{Cn} , VAL_{In} , VAL_{An})$

Criticità della base dati rispetto alle componenti CIA

Considerando la componente di rischio dovuta alla confidenzialità:

$R_{Cn} = f (\text{suscettibilità} , \text{valore}) = S_{Cn} * VAL_{Cn}$

Nota: abbiamo definito il rischio come prodotto tra suscettibilità e valore dell'informazione (assumendo proporzionalità lineare)

IT Security Risk Analysis



$\underline{S}_n = (S_{Cn} , S_{In} , S_{An})$ suscettibilità associata alla base dati n-esima

$$\begin{aligned} S_{Cn} &= (M_1 * V_{1n} * C_{C11} + M_1 * V_{2n} * C_{C12} + \dots + M_m * V_{vn} * C_{Cmv}) \\ &= \underline{M} * \underline{C} * \underline{V}_n \end{aligned}$$

\underline{C}_C rappresenta la matrice delle correlazioni tra le vulnerabilità e le minacce per la confidenzialità: ogni componente mette in relazione il “danno” che la singola minaccia può fare sfruttando la singola vulnerabilità.

Nota: per i componenti della suscettibilità abbiamo assunto una proporzionalità lineare tra valori delle minacce, delle vulnerabilità e delle correlazioni.

Per S_{In} e S_{An} si ragiona analogamente.

IT Security Risk Analysis



Riepilogo input del modello:

- Minacce
- Vulnerabilità
- Correlazione minacce – vulnerabilità
- Criticità delle basi di dati rispetto a CIA

Riepilogo output del modello.

- Rischio collegato alle basi di dati

IT Security Risk Analysis

Definizione soglie e taratura



Il modello fornisce valori numerici che devono essere interpretati in un linguaggio comprensibile dal management aziendale. Occorre definire delle soglie numeriche che permettano di classificare il rischio:

- Basso
- Medio
- Alto

Per completare il modello occorre svolgere una complessa attività di taratura. Il modello viene alimentato con scenari tipo, per i quali è definibile la suscettibilità ed il rischio, e se ne verifica la coerenza.

La taratura deve essere effettuata prima di fornire il modello agli utenti per la rilevazione dei valori di minaccia e di criticità.

IT Security Risk Analysis



Utilizzando gli strumenti prodotti viene svolta l'attività di raccolta delle informazioni sul campo.

I dati alimenteranno il modello per fornire una misurazione del grado di rischio per le varie basi di dati aziendali.

IT Security Risk Analysis



Da un'attività come quella descritta il management può ottenere importanti informazioni utilizzabili, ad esempio, per decidere investimenti nel settore della sicurezza informatica.

I risultati ottenuti sono “oggettivati” da una metodologia.

IT Security Risk Analysis

Analisi di rischio “quantitativa”

Il processo mostrato fino ad ora permette di dare un giudizio in termini qualitativi del grado di sicurezza delle informazioni, ma non riesce a produrre un bilancio economico dell’impatto del rischio e del costo per l’attivazione e la gestione del controllo.

Il significato di una affermazione quale “il rischio è ALTO” può non essere immediatamente compresa dal management.

Il management ha bisogno di sentirsi dire cosa comporta in termini economici il rischio.

L’analisi di rischio quantitativa cerca di rispondere a questa esigenza.

IT Security Risk Analysis

Elementi essenziali dell'approccio quantitativo sono:

➤ conversione in termini monetari del valore associato alle risorse

✓ non è complesso

➤ considerazione delle minacce in termini di frequenza (eventi / anno)

✓ è complesso

Per riuscire a ragionare in termini di frequenza sarebbe necessario possedere una base di conoscenza che collegasse gli eventi agli impatti economici

→ Le aziende, se possono, evitano di dare notizie di perdite collegabili a lacune nei controlli di sicurezza delle informazioni.

Materiale per consultazione

- In relazione ai problemi della risk analysis quantitativa

<http://www.itaudit.org>

Will Ozier “Risk Metrics Needed for IT Security”