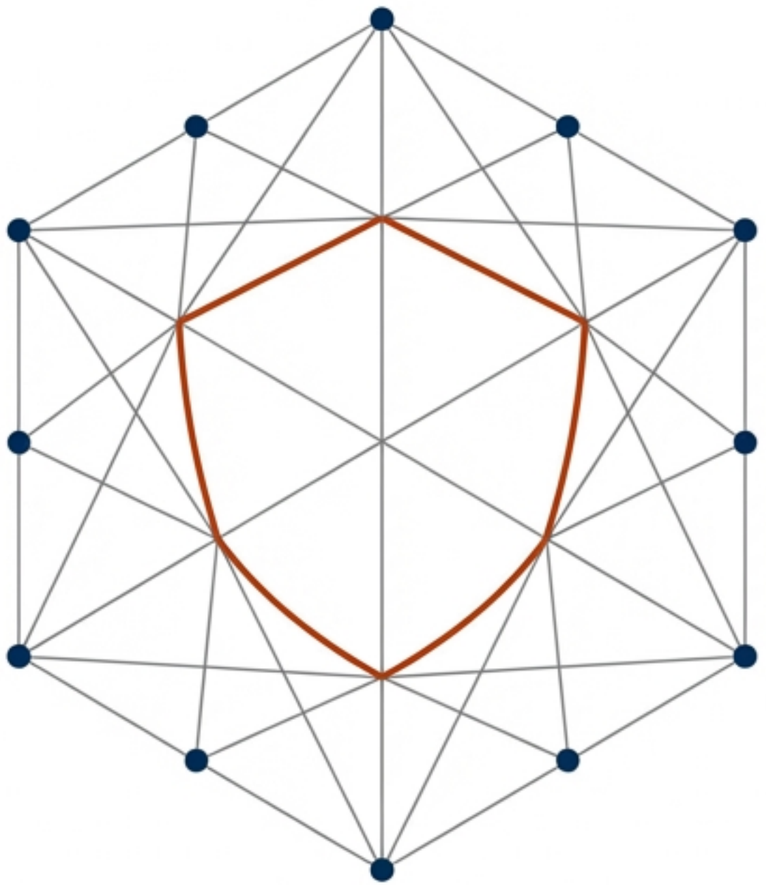
Il Contesto dell'IT Risk Management: Dalla Corporate Governance ai Controlli Operativi



Analisi dei rischi, quadri normativi e modelli di governo dei sistemi informativi.

L’Evoluzione della Responsabilità Aziendale

- La gestione dei rischi IT non è più una competenza esclusiva dei tecnici, ma una responsabilità diretta degli organi di governo (Board).

Dovere di Diligenza

Necessità di tutelare il valore per gli azionisti e gli interessi degli stakeholder.

Conseguenze

La mancata identificazione delle minacce porta a crisi aziendali e pressioni dirette sui vertici.

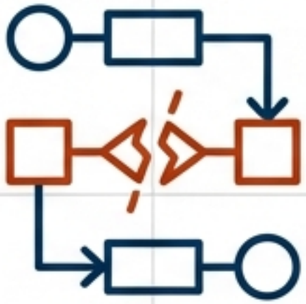
Evidenze Empiriche: L'Impatto Economico e Operativo

Sony Corporation (2011)

Evento: Attacco al PlayStation Network, furto di dati sensibili (nomi, carte di credito).

Impatto: Blocco attività globali, danno stimato di 14 miliardi di Yen (ca. **122 milioni di Euro**), *class action* e danno reputazionale.

Poste Italiane (2011)



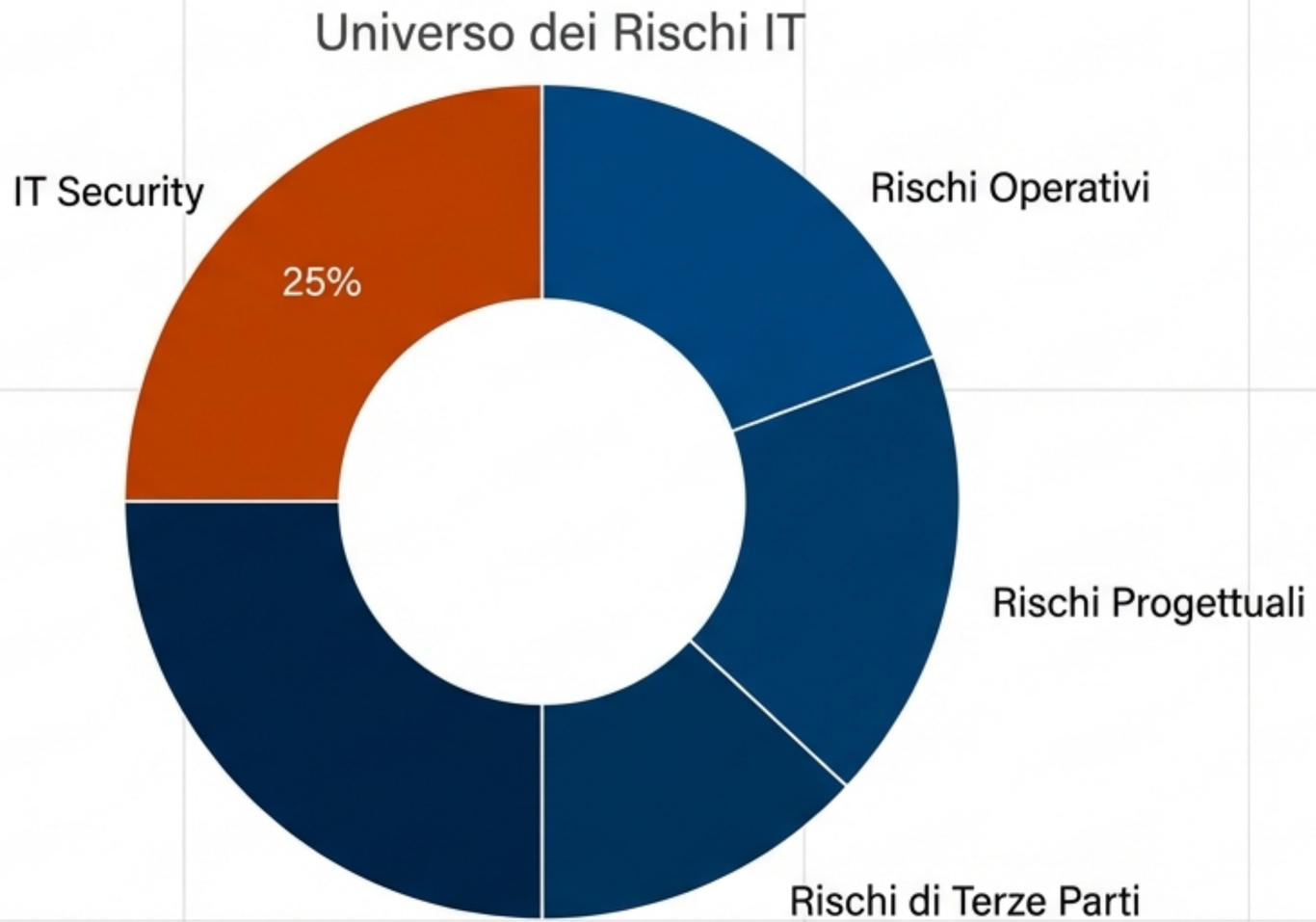
Evento: Progetto di centralizzazione dei sistemi informatici.

Impatto: Paralisi operativa di migliaia di sportelli, seduta straordinaria del CdA, procedure di risarcimento clienti.

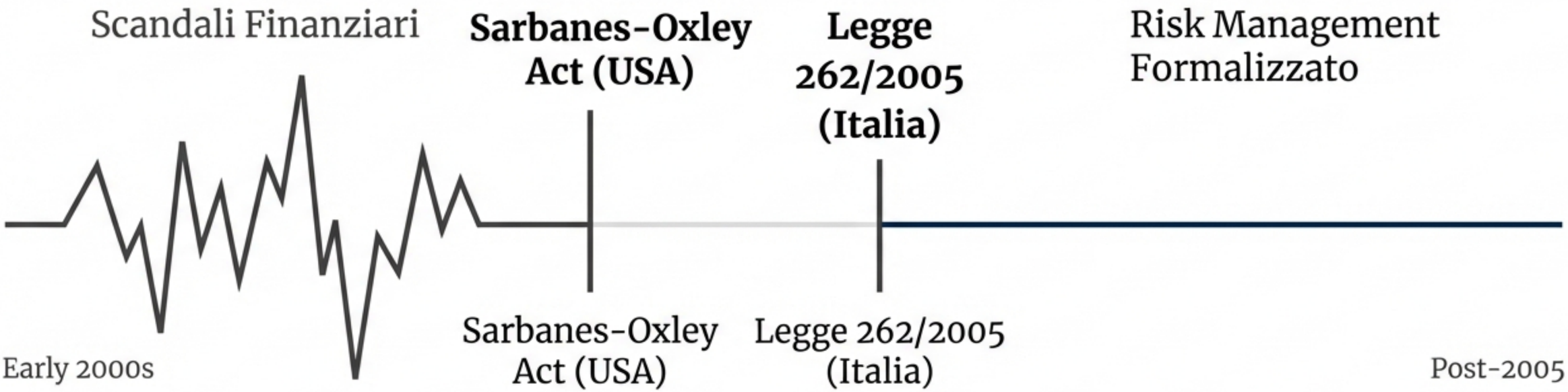
Oltre la Sicurezza Informatica: La Tassonomia delle Minacce

Un errore comune è focalizzarsi solo sulla protezione dei dati. I rischi IT sono sistemici.

- **Rischi Operativi**: Gestione delle risorse umane e finanziarie.
- **Rischi Progettuali**: Gestione di progetti ad alto contenuto tecnico e disegno di architetture applicative.
- **Rischi di Terze Parti**: Relazioni con soggetti esterni e outsourcing (impatto sull'operatività).



Il Panorama Normativo e la Risposta dei Regolatori



Obiettivo Normativo: Obbligo per il *Board* di certificare l'adeguatezza dei controlli interni e la correttezza dell'informativa finanziaria (*Financial Reporting*).

Le Patologie del Risk Management Tradizionale

Approccio a Silos

Iniziative frammentate e settoriali senza visione d'insieme.

Reattività

Azioni basate sulla reazione all'evento piuttosto che sulla prevenzione.

Ridondanza

Duplicazioni di metodi e mancanza di un presidio centrale.

Mancata Condivisione

Difficoltà nel condividere buone prassi e misurare le prestazioni.

Enterprise Risk Management (ERM): Il Paradigma COSO

La Gerarchia del Governo Aziendale

Distinzione Cruciale: Una buona IT Governance gestisce i rischi ‘naturalmente’. Tuttavia, un buon IT Risk Management *non* implica automaticamente una buona Governance.

Fallimento della Governance: Il Caso Royal Bank of Scotland (RBS)

2012

Blocco dei prelievi/pagamenti. Causa: upgrade sistema mainframe (architettura CA7).

2013

Nuovo blocco durante lo shopping natalizio. Stesso sistema, stesso staff.

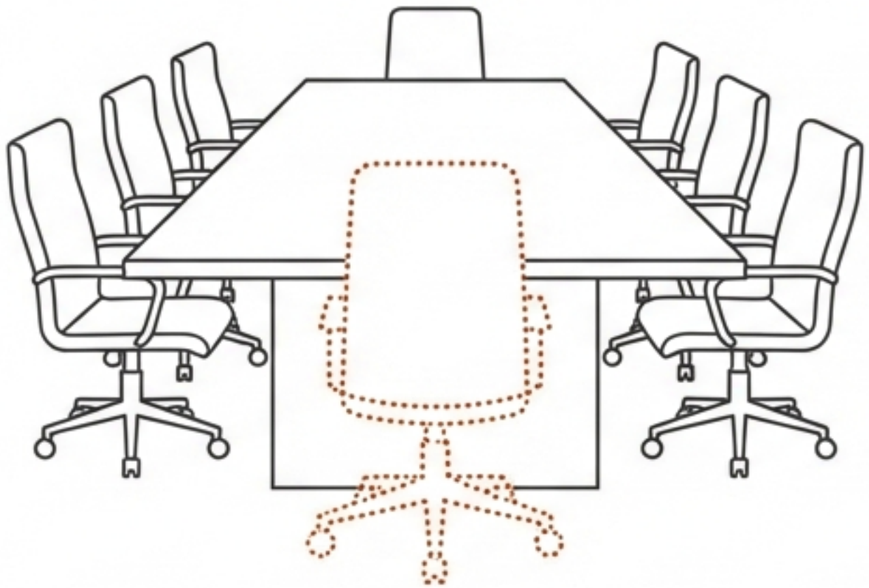
Ammissione di decenni di negligenza negli investimenti.

2014

Ulteriore guasto e multa di 50 milioni di sterline.

Lezione: Il problema non era solo tecnico, ma strategico: l'assenza di una governance in grado di pianificare la modernizzazione delle infrastrutture.

L’Assenza di Responsabilità Strutturale: Sony (2012)



Il Gap di Governance

Prima del giugno 2012, in Sony **non esisteva la figura del CISO** (Chief Information Security Officer).

Narrativa

Estate 2012: Attacchi hacker ripetuti al PlayStation Network. Intervento del CdA con scuse pubbliche per arginare il crollo del titolo.

Takeaway

Il sistema di IT Governance è il presupposto indispensabile; senza definire i ruoli, l'IT Risk Management non può funzionare.

Definizioni Accademiche di IT Governance

IT Governance Institute

Responsabilità del Board per assicurare che l'IT supporti la strategia aziendale.

Van Grembergen

Meccanismi di delega per allineare strategia IT e strategia di business.

Severino Meregalli (SDA Bocconi)

Logiche e strumenti per creare un "allineamento naturale" dell'IT alle esigenze aziendali in condizioni di economicità.

Funzione Core : Definire i diritti decisionali ("Chi decide cosa") e i livelli di tolleranza al rischio.

I Controlli nel Framework COSO

Prospettive di Gestione: Chi Possiede il Rischio?

Business Owned

(Prospettiva Application Controls)

L'IT è una risorsa pervasiva di business; il rischio è del processo aziendale supportato.

Unit Risk Owner

(Prospettiva IT General Controls)

La funzione IT è un'unità aziendale specifica che gestisce i propri rischi interni (infrastruttura, sviluppo).

Enabler

(Prospettiva Strumentale)

L'IT fornisce strumentti software a supporto del processo di ERM.

IT Risk Management: Una Definizione Operativa

Definizione

Gestione del rischio di business collegato all'utilizzo, proprietà, adozione e influenza degli strumenti IT nell'azienda.

****Focus del Corso****
In questo contesto, assumeremo la prospettiva dell'IT come **Unit Risk Owner.**

****Obiettivo****
Superare il deficit di attenzione e integrare la gestione del rischio IT nei processi decisionali.

Conclusioni e Punti Chiave

1. **Responsabilità**: Il rischio IT è una questione di Corporate Governance, non solo tecnica.
2. **Integrazione**: L’approccio ERM (COSO) supera la logica a "silos" frammentata.
3. **Gerarchia**: Una solida IT Governance è il prerequisito per un efficace IT Risk Management.
4. **Applicazione**: Necessità di bilanciare Application Controls (Business) e IT General Controls (Infrastruttura).

Il valore dell'impresa dipende dalla capacità di governare la tecnologia che lo supporta.