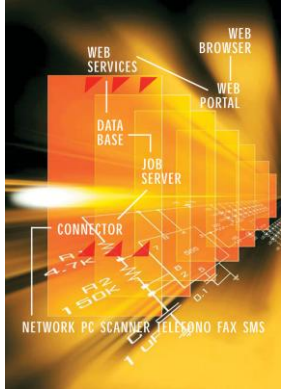
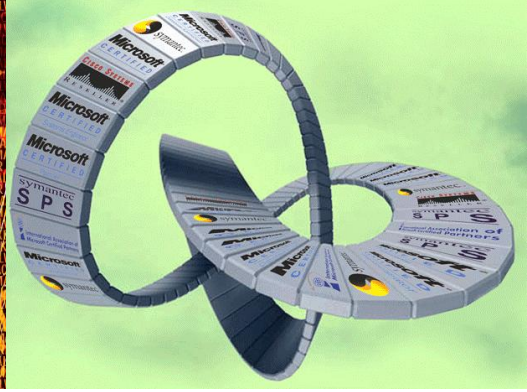
KBE





GOVERNANCE, RISCHI E COMPLIANCE: UNA VISIONE DELLA SICUREZZA DI TIPO CONVERGENTE

ABI EVENTI

ABI Associazione Bancaria Italiana

Roma – 6 Giugno 2013

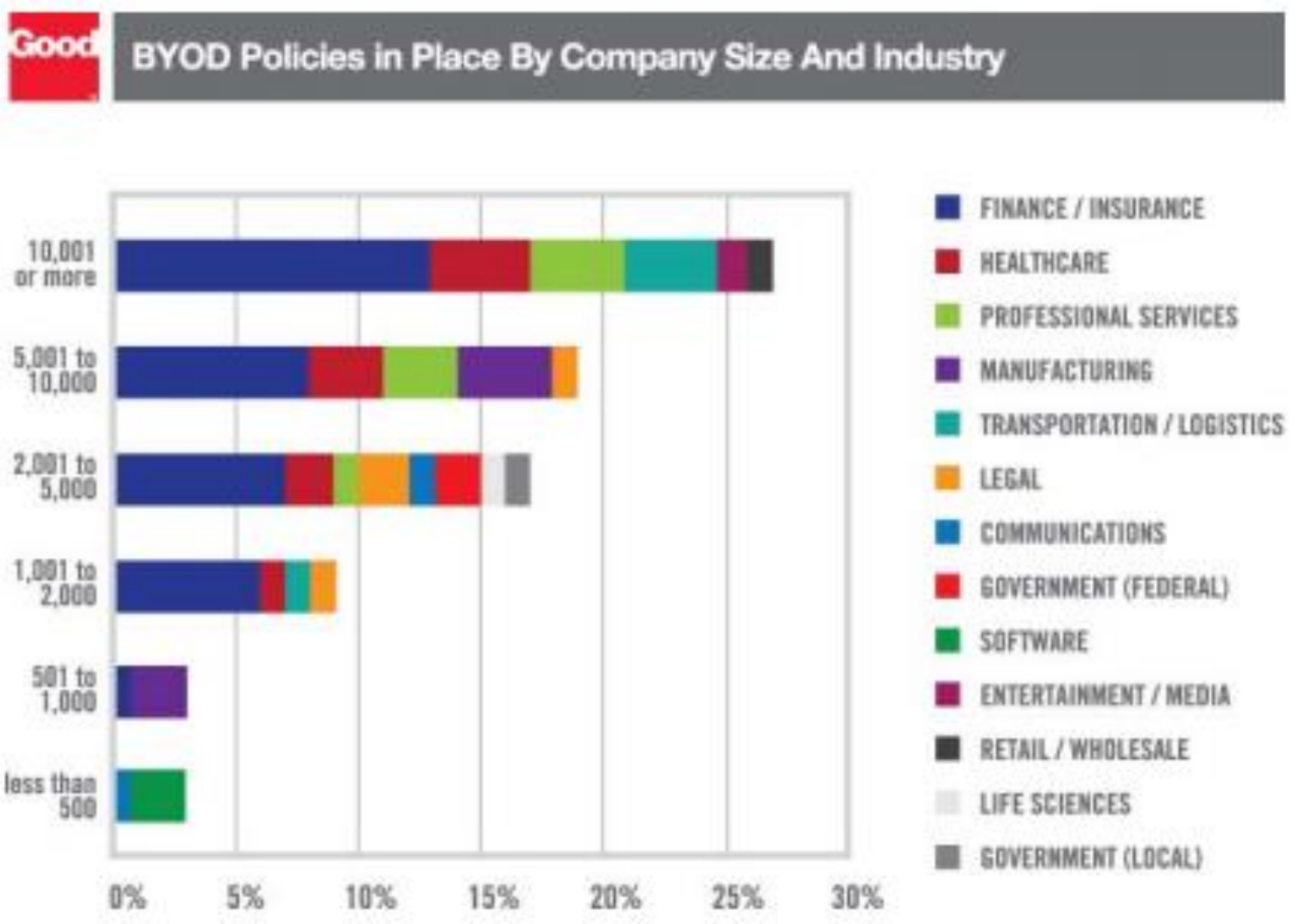
Fabio Rovati, CISSP, CISSP-ISSAP, CISM – Security Practitioner @ KBE srl

Sfide

Sfide

- Compliance Vs Governance
- Cyber threat Vs Nuovi canali
- Frodi Vs Operatività
- Rischi Vs Opportunità

Sfide


Good
BYOD Policies in Place By Company Size And Industry
10,001 or more
5,001 to 10,000
2,001 to 5,000
1,001 to 2,000
501 to 1,000
less than 500
0%
5%
10%
15%
20%
25%
30%
FINANCE / INSURANCE
HEALTHCARE
PROFESSIONAL SERVICES
MANUFACTURING
TRANSPORTATION / LOGISTICS
LEGAL
COMMUNICATIONS
GOVERNMENT (FEDERAL)
SOFTWARE
ENTERTAINMENT / MEDIA
RETAIL / WHOLESALE
LIFE SCIENCES
GOVERNMENT (LOCAL)

Perché è difficile la Sicurezza

Primo «successo» : la sicurezza per controlli

Perché è difficile la Sicurezza

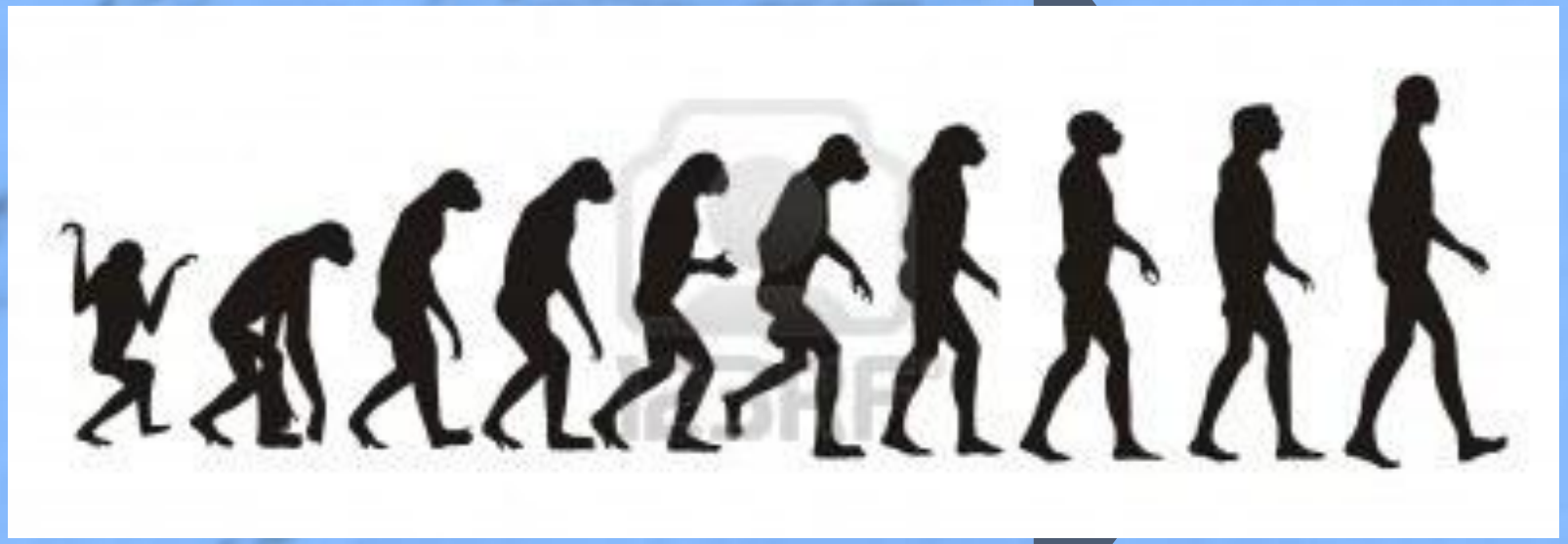
Secondo «successo»: la sicurezza gestita

Persone

- Difesa di tipo multi-layer
  - Livello Perimetrale
  - Livello Network
  - Livello Device
  - Livello Applicazioni
  - Livello Dati (documenti e database)

Tipical Information Security approach

Persone



- Personal Security Layer

Livello della Persona

Enterprise Security Risk Management

- ESRM è un approccio olistico ed integrato che opera ad identificare e mitigare tutti i rischi che l'azienda deve affrontare, indipendentemente dall'area coinvolta.


ATTITUDE
CAREER
ARTISTIC
MY GOALS
FAMILY
PUBLIC SERVICE
PLEASURE
PHYSICAL
FINANCIAL

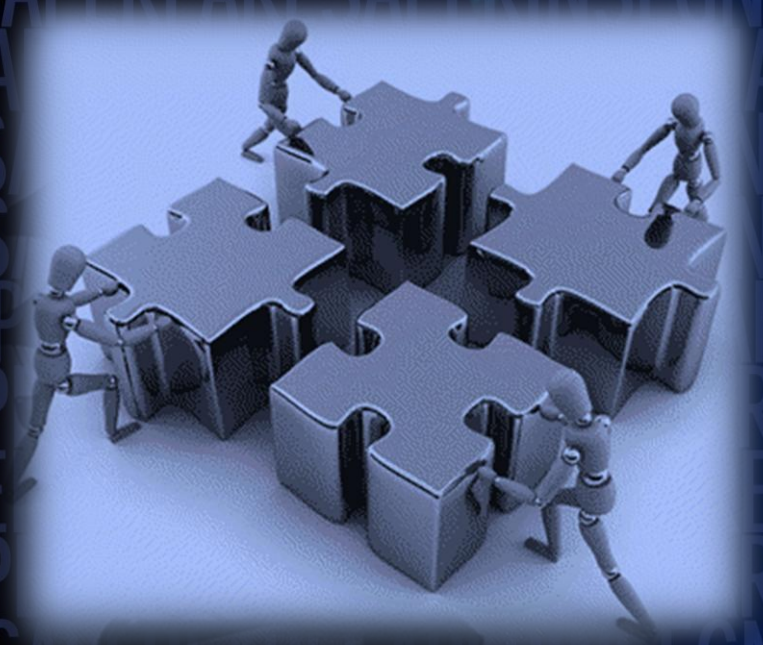
Goal

Obiettivi (della security)

- Rispetto di normative e regolamentazioni
- Framework
- Salvaguardare la confidenzialità delle proprie risorse (classificazione)
- Gestione delle complessità
- Approccio GRC convergente
- Risk design e framework

Obiettivi (della presentazione)

- Vision
- Roadmap



Strategie

Vision

- Approccio basato sui rischi e non sui controlli
- Gestione olistica delle persone
- Positiva cultura della sicurezza
- Puntuale responsabilità del rischio
- Trasparenza e legalità

Case History

La Signora R, di circa quarant'anni, dipendente con livello da «impiegato», lavorava per la stessa azienda da sempre.

Il suo capo, Signor A, era più giovane di dieci anni ed era visto nell'azienda come l'astro nascente. Nella sua valutazione annuale, il manager, il sig. A descrisse la signora R come «resistente al cambiamento» e una «lavoratrice di medio livello».

La Signora R si lamentò con il suo precedente responsabile, il Signor B. dicendo che il suo diretto superiore, signor A, non le aveva dato alcun credito per la qualità del suo lavoro, o per la sua esperienza. Descrisse l'atteggiamento del suo nuovo capo come «sessista e tipico del bullismo».

Dopo qualche discussione, il signor B le disse che, anche se riconosceva l'importante contributo dato nel corso degli anni, non riusciva a sostenere la sua denuncia. Il Signor B, invece, spinse la signora R a migliorare la sua relazione con il suo manager e di ampliare la conoscenza dell'azienda per provare ad ottenere una migliore comprensione di come era cambiata.

Nelle settimane successive, il sistema di controllo accessi rilevò che la sig.ra R aveva cambiato il suo metodo di lavoro, lavorando più ore ed spesso risultò l'ultima persona a lasciare l'ufficio. Il sistema di monitoraggio degli accessi logici rilevò che la sig.ra R ebbe accesso a dati aziendali che avevano poco a che fare con il suo lavoro e molte delle sue ricerche sui database apparvero essere casuali e non correlate. Queste ricerche non violavano nessuna policy aziendale, ma il volume di informazioni acquisite potevano essere di notevole aiuto per un concorrente.

Processo di gestione

Roadmap per applicare l'ESRM

Policy trasparenti	Unico responsabile del rischio di persone	Istruire e Far crescere ottimi responsabili	Imporre un efficace sistema di controllo accessi	Applicare tre prerequisiti	Collezionare, aggregare e analizzare i dati personali	Applicare un piano di comunicazione prestabilito
• Essere trasparente • Sviluppare e applicare policy trasparenti • Tenere informati e consentire l'accesso al monitor di protezione • Ottenere il supporto dei dipendenti	• Assicurare un approccio olistico di tutti i rischi	• Responsabili di ufficio • HR • Direzione	•Fisico •Logico •Privilegi elevati	• Gestire gli asset • Gestire le identità e gli accessi • Gestire i rischi	• Accedere ai dati sensibili solo in accordo con le policy	•Istituire training e programmi di consapevolezza •Focalizzarsi sui rischi e su casi pratici •Combattere i crimini

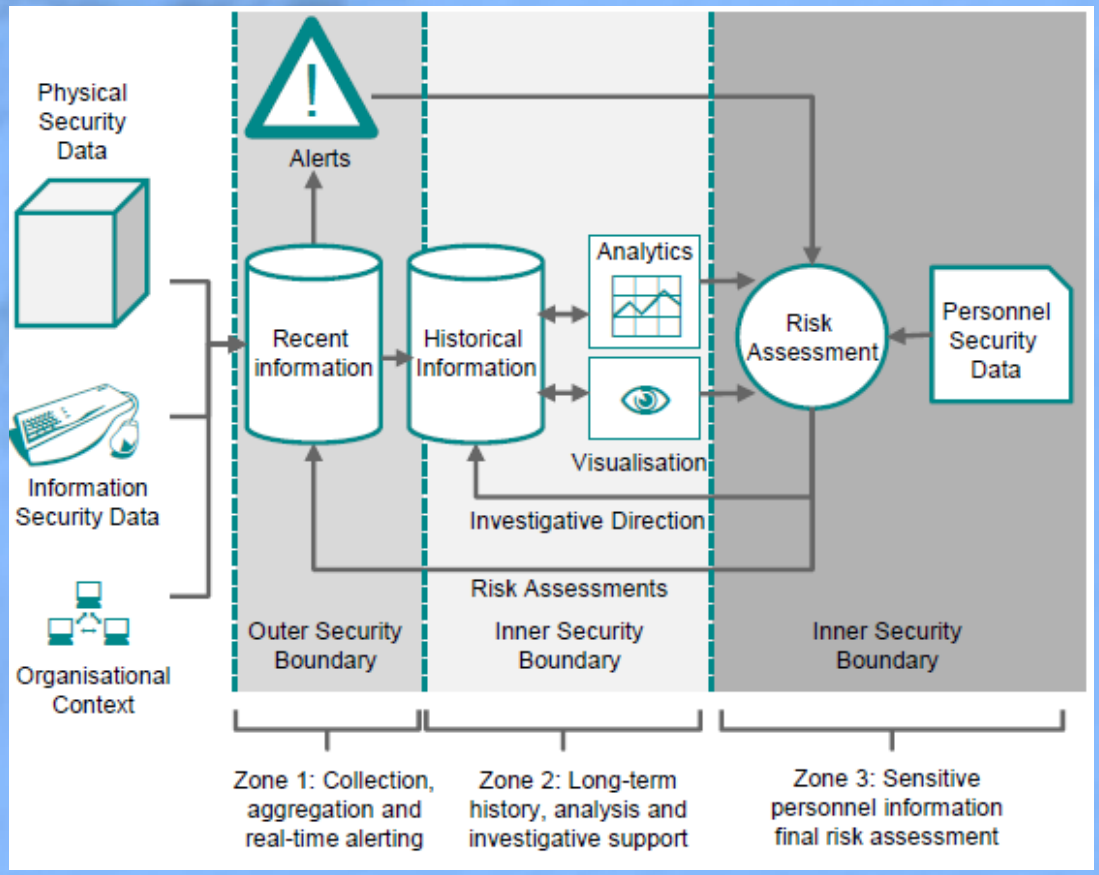
ESRM Tools

Monitoraggio di protezione

Collezione dei log in real time

Aggregazione dei log per analisi di lungo termine

Risk Assessment basato su dati personali



Considerazioni

Cosa si può dare al capo

- Protezione degli asset più a rischio
- Priorità nella remediation
- Metriche per misurare l'ambiente e le performance
- Soluzione integrata di
  - Governance
  - Approccio olistico
  - Risk Management
  - Framework e standard
- Ambiente sereno
- Riduzione dei costi di gestione del rischio

Strategia vs Risultati

Anche se è bello avere una strategia, poche volte si guarda ai risultati

Winston Churchill

Tutti hanno una strategia, fino a quando non ricevono un pugno in faccia

Iron Mike Tyson

Domande e Risposte

Risposte (scegliere la più opportuna in base alla vostra domanda):

- **Non Lo So**
- **Non Si Può**
- **Non Funziona**

KBE

KBE Intelligence

Viale Sabotino 19/2

20135 – Milano

www.kbe.it

kbe@kbe.it