Compliance normativa e tecnologie informatiche: un sistema in evoluzione

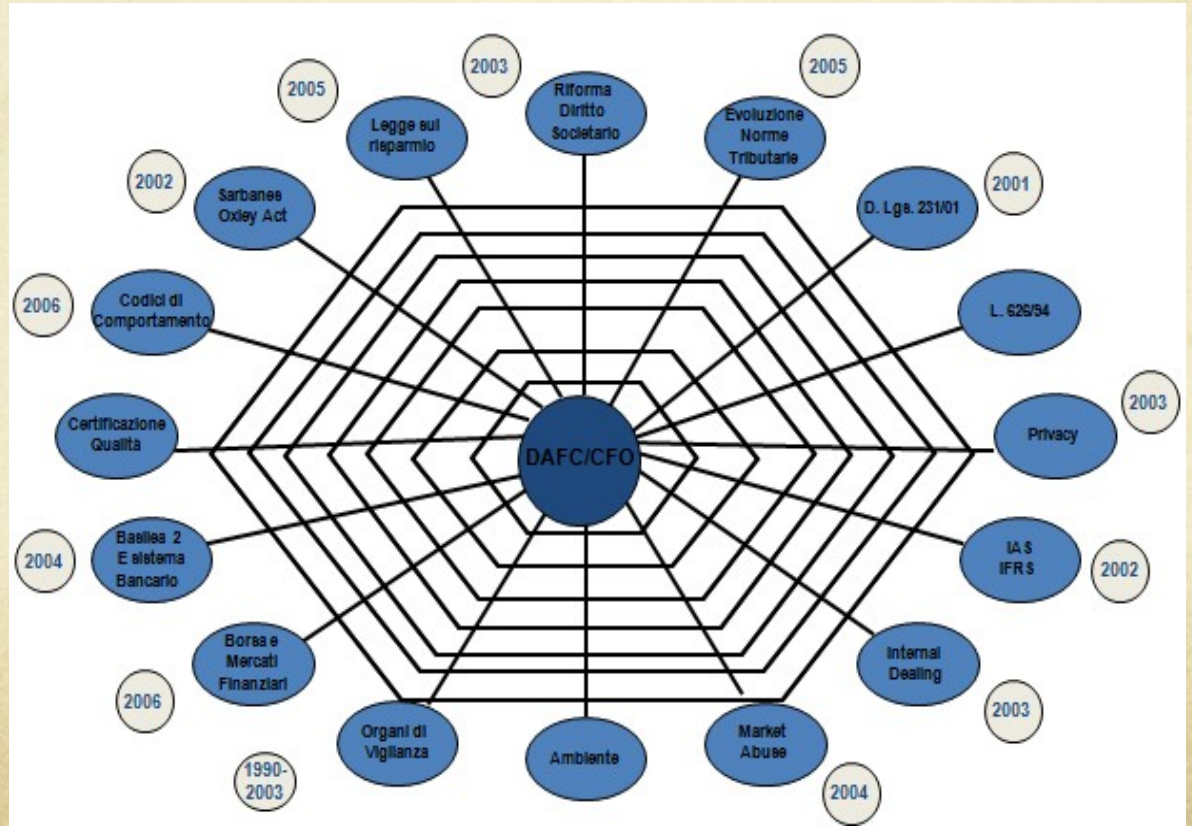
Prof. Ing. Claudio Cilli
cilli@di.uniroma1.it
http://dsi.uniroma1.it/~cilli

La maggior astuzia del Diavolo è convincerci che non esiste
Charles Baudelaire, Litanie a Satana

Corruptissima re publica plurimae leges
Tacito, Annales, Libro III, 27

L'evoluzione della normativa societaria

- La produzione normativa degli ultimi anni ha posto particolare enfasi sull'adeguatezza del sistema di controllo interno aziendale e quindi sulla capacità da parte degli organi societari di definire adeguati sistemi di controllo che garantiscano il rispetto delle politiche e procedure aziendali da un lato e dall'altro il raggiungimento degli obiettivi di business prefissati



Quando la normativa insegue...

...il ritardo è evidente

- La privacy è senza dubbio uno dei temi più affrontati quando si parla di riprese aeree con drone. La massiccia diffusione degli Apr ha portato con sé una serie di preoccupazioni. Una di queste riguarda senza dubbio la riservatezza. Ma cosa è lecito riprendere in concreto?

- La base, per quel che riguarda le riprese aeree con drone, è rappresentata naturalmente dal Regolamento ENAC. La normativa stabilisce, oltre alla necessità di indicare nel modulo di autorizzazione l'eventuale trattamento di dati personali, che l'operatore deve rifarsi alla legge 196/2003 (Codice per la protezione dei dati personali). Il riferimento, in particolare, è l'articolo 3 che stabilisce che "i sistemi informativi e i programmi informatici sono configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi".

- La domanda fondamentale, però, riguarda cosa si può e cosa non si può riprendere. Preliminare alla risposta, bisogna sapere che, sempre il Codice, all'articolo 5 stabilisce che le normative sulle privacy si applicano solo nel caso in cui le foto o i video siano destinati alla pubblicazione, su qualunque mezzo.

- Riassumiamo. L'operatore deve fare in modo di ridurre al minimo l'utilizzazione di dati personali e identificativi. Contemporaneamente, nel caso decida di tenere per sé le immagini, non ha particolari limitazioni per quanto riguarda la privacy.

Droni invasivi

- Il punto, ora, è capire come si può fare a riprendere una persona e pubblicarla. Nel caso di un ritratto (occasione rara nel caso di riprese aeree con drone) c'è bisogno di una liberatoria firmata da un diretto interessato.

- Nel caso di immagini paesaggistiche, se una foto comprende delle persone, e la medesima non rientra nella categoria ritratto, la foto (o il video) può essere esposta o pubblicata se non reca pregiudizio al decoro o alla reputazione della persona, secondo l'articolo 10 del Codice Civile.

- Una sentenza della Corte di Cassazione (47165/2010) ha chiarito ulteriormente la situazione. La disposizione ha stabilito che una normale ripresa all'esterno in cui siano coinvolte persone può diventare illecita "quando si adottano sistemi per superare quei normali ostacoli che impediscono di intromettersi nella vita privata altrui".

- Tradotto, non si possono superare barriere di abitazioni o di residenze private, ma si possono riprendere persone in luoghi che siano visibili pubblicamente come, ad esempio, il balcone di un appartamento.

I reati informatici

Per **crimine informatico** intendiamo:

ogni comportamento previsto e punito dal codice penale o da leggi speciali in cui qualsiasi strumento informatico o telematico rappresenti un elemento determinante ai fini della qualificazione del fatto di reato

Si utilizza il termine **"reato informatico"** per indicare qualsiasi condotta realizzata per mezzo delle nuove tecnologie o comunque rivolta contro i beni informatici, sanzionata dall'ordinamento penale. Può essere considerato reato informatico tanto la frode commessa attraverso il computer che il danneggiamento del sistema informatico

Una definizione "*dottrinaria*" di crimine informatico è:

"crimine nel quale un sistema di elaborazione o una sua parte ricopre uno dei seguenti ruoli:

- **oggetto** (ciò include la distruzione o la manipolazione dell'elaboratore, dei dati e dei programmi in esso contenuti e delle relative apparecchiature di supporto)
- **soggetto** (quando l'elaboratore è il luogo, il motivo o la fonte del crimine)
- **strumento** (quando ciò che avviene in relazione all'elaborazione non è di per sé illegale, ma serve a commettere crimini di altro tipo, es. sabotaggio). In pratica un sistema di elaborazione, o ciò che viene prodotto dall'elaboratore, è usato come mezzo per compiere frodi, sabotaggi, falsificazioni"

I penetration test

- Eseguire regolarmente Penetration Test aiuta le organizzazioni a scoprire i punti deboli della sicurezza della rete, che possono portare a sottrazione di dati o ad apparecchiature compromesse da exploit, virus, trojan, attacchi Denial of Service ed altre intrusioni.
- Rileviamo subito l'assenza di norme che si occupino nello specifico di questa categoria, ma chiariamo sin da subito che nessun operatore ne ha mai sentito la mancanza e che non si può parlare di vuoto normativo.
- Rileviamo subito l'assenza di norme che si occupino nello specifico di questa categoria, ma chiariamo sin da subito che nessun operatore ne ha mai sentito la mancanza e che non si può parlare di vuoto normativo.

La natura del contratto di penetration test

- Contratto atipico misto:
  - Basato su appalto o contratto d'opera.
  - Obbligazione di mezzi.
  - Organizzazione dei mezzi in capo al tester.
- Rileviamo subito l'assenza di norme che si occupino nello specifico di questa categoria, ma chiariamo sin da subito che nessun operatore ne ha mai sentito la mancanza e che non si può parlare di vuoto normativo.

Privacy e sicurezza dei dati di terzi

- Il Codice in materia di protezione dei dati personali impone al c.d. *titolare del trattamento* degli obblighi(generalmente quelli di un comportamento lecito e corretto, quelli di informativa, un'adeguata custodia e sicurezza).
- Problema: effettuando un PT un terzo estraneo e non autorizzato *dall'intestatario al trattamento* potrà operare sui dati col rischio che possa appropriarsene o disperderli.
- Il tentativo di considerare il tester come *incaricato del trattamento.*
- La *strada del Bilanciamento* degli interessi.
- La responsabilità presunta ex. Art. 2050 c.c.

Aspetti penali

- Il tester può essere esposto a responsabilità penali per vari capi di reato. Si ricordi che l'attività stessa del test integrerebbe una condotta criminosa che deve essere legittimata dalla scriminante di cui all'art. 50 c.p., ovvero il consenso dell'avente diritto. Caratteristiche del consenso devono essere la spontaneità, l'attualità e la disponibilità del diritto. Come già detto, è prevista una necessaria forma, ma anche in questo caso la forma scritta è imposta dalla dovuta cautela di fronte ad una così grave responsabilità.

- Discostandosi dal proprio incarico, il tester può commettere alcuni reati che andiamo ad elencare:
  - Art. 50 c.p. "Non è punibile chi lede o pone in pericolo un diritto, col consenso della persona che può validamente disporne"
  - Art. 615 ter c.p. "chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni" – Aggravante: essere amministratore di sistema
  - Furto di dati (624 c.p.)
  - Trattamento illecito dei dati (art. 167 e 168 Codice in materia di protezione dei dati personali

Aspetti penali

- **Danneggiamento di sistema informatico (635 bis)**: Il reato in questione va ad estendere la punibilità previsto per il danneggiamento tradizionale anche a quello relativo a beni informatici.
  - Il tester potrebbe incappare in una responsabilità del genere ogni qualvolta che modifichi il sistema fuori dai limiti del suo mandato. Ci si potrebbe chiedere se la responsabilità penale da danneggiamento può derivare anche da semplice colpa: la giurisprudenza ha dato risposta negativa al quesito, facendo salva però l'azione da responsabilità civile.

Honeypot

- “Risorsa il cui valore risiede nell’essere rilevata, attaccata e compromessa” (Lance Spitzne)
- Possiamo considerare gli obiettivi un Honeypot come:
  - Disporre di un sistema in grado di essere rilevato, attaccato e compromesso.
  - Registrare tutte le attività intrusive per acquisire informazioni sugli strumenti e le strategie impiegate
- Privacy: il problema è superabile, in quanto la norma che punisce la raccolta e il trattamento dei dati personali, non compre i casi in cui ci si riferisce a dati intercettati attraverso un proprio host bucato e utilizzato per fini non commerciali o in altro modo illecito.
- Si può parlare di agente provocatore?

Problemi legali

- Come anticipato, nella letteratura riguardante gli HoneyPot, dubbi sulla pratica sono stati riferiti agli aspetti legali. Alcuni autori infatti si son chiesti se il creare un oggetto destinato subire degli attacchi potesse essere, in alcuni casi, considerato come una provocazione a compiere i reati di accesso abusivo o di danneggiamento a sistemi informatici.

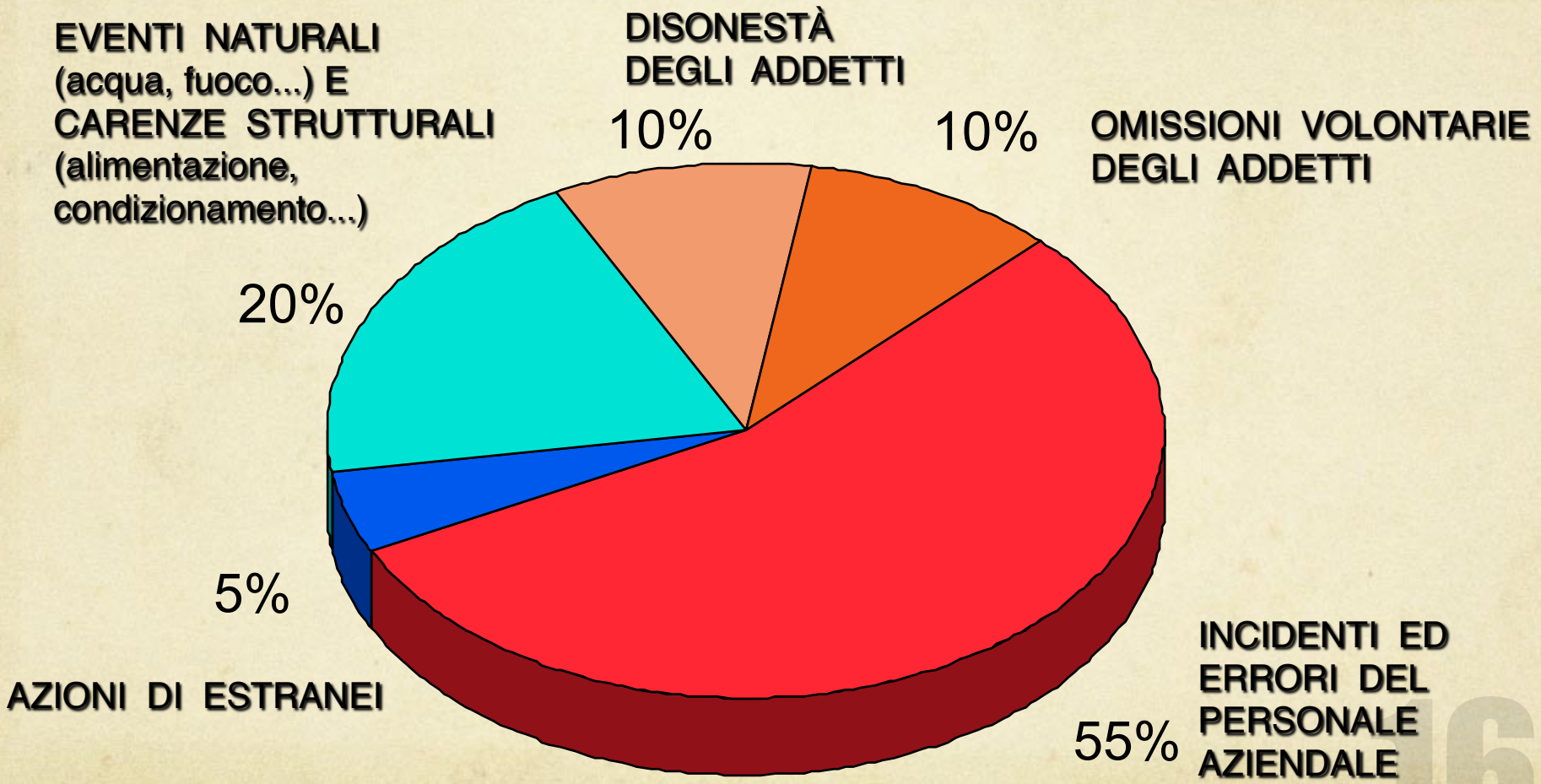
- La letteratura in questione si riferisce al principio che chiunque faccia sorgere o accrescere in altri un proposito di reato soggiace alla stessa, vale a dire quell'ipotesi che i giuristi chiamano “Concorso morale di persone nel reato” . A questo si aggiunge una particolare ed ambigua categoria del concorso morale che è l'agente provocatore. Questo è definito come colui che istiga la commissione del reato per poter poi chiedere l'incriminazione dell'autore.

- Quelli riguardanti gli HoneyPot non sono i primi dubbi che questi concetti han posto ai tecnici del diritto. A riguardo infatti mancano dei precisi riferimenti normativi: sono figure estratte dalla giurisprudenza sulla base di altre norme, con la conseguente carenza di certezza.

Conclusioni...non conclusive

- La BBC ha condotto un importante esperimento realizzando un Honeypot. Collegata la macchina ad internet, senza alcuna sollecitazione da parte della BBC, questa è stata attaccata in media ogni 15 minuti.
- Quindi come si è visto, nonostante ci sia tanta letteratura e giurisprudenza che affronta l'argomento Honeypot, non si è riusciti a rispondere in modo netto, univoco sulla opportunità o meno dell'uso di queste risorse.
  - Se consideriamo punibile un'HoneyPot dovremmo considerare punibile anche un uomo che, sapendo di dover attraversare una zona malfamata anziché indossare un gioiello di valore ostentasse una buona imitazione e questo gli venisse rubato...
  - ...ma qualcuno potrebbe obiettare che questa persona indosserebbe questo gioiello falso proprio allo scopo di farselo rubare e che quindi ciò sia da considerarsi istigazione
- Quindi? Nessuna certezza!

Incidenza dei danni per tipologia



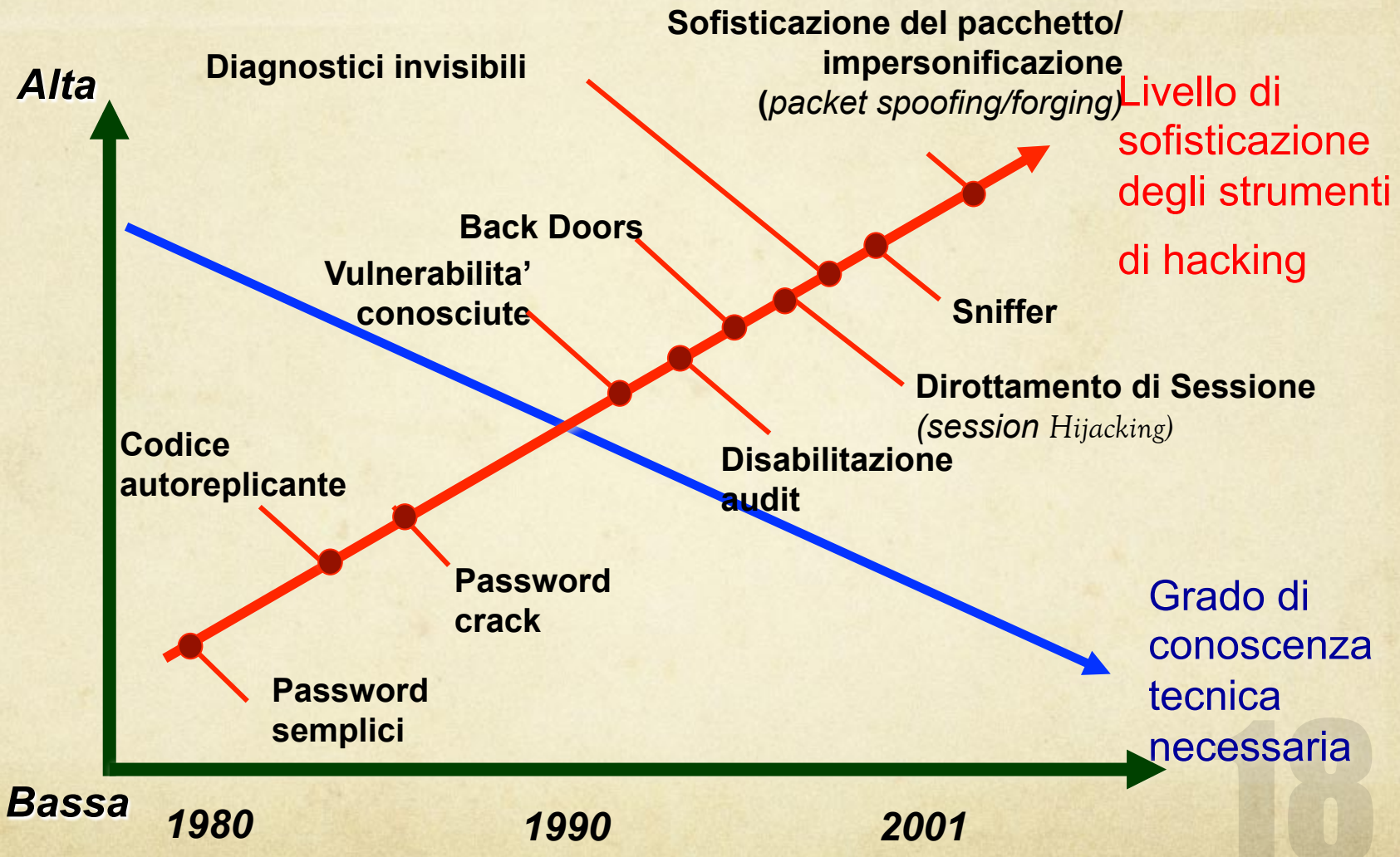
L'approccio metodologico: principali normative e requisiti

	Analisi dei rischi	Scoping	Documentazione e Testing dei controlli	Remediation/Azioni di miglioramento	Monitoraggio
Legge 262/05	✓	✓	✓	✓	✓
D. Lgs. 231/2001	✓	✓	✓	✓	✓
Privacy e data protection	✓	✓	✓	✓	✓
TUF e "market abuse"		✓	❖	❖	❖
Normative Verticali di Settore	✓	✓	✓	✓	✓
D. Lgs. 81/2008	✓	❖	❖	✓	✓
Testo Unico Ambiente	✓	✓	❖	❖	✓
Qualità/Norme ISO	❖	✓	❖	✓	✓

❖ Applicabile nei limiti specifici della normativa.

Per poter gestire le diverse normative è necessario partire con l'identificazione di "driver" comuni alle diverse leggi. Dall'analisi effettuata emerge che l'analisi dei rischi, la definizione del perimetro di analisi (scoping), la documentazione e il testing dei controlli, l'attività di remediation e il monitoraggio dei rischi e dei controlli sono attività comuni a quasi tutte le normative

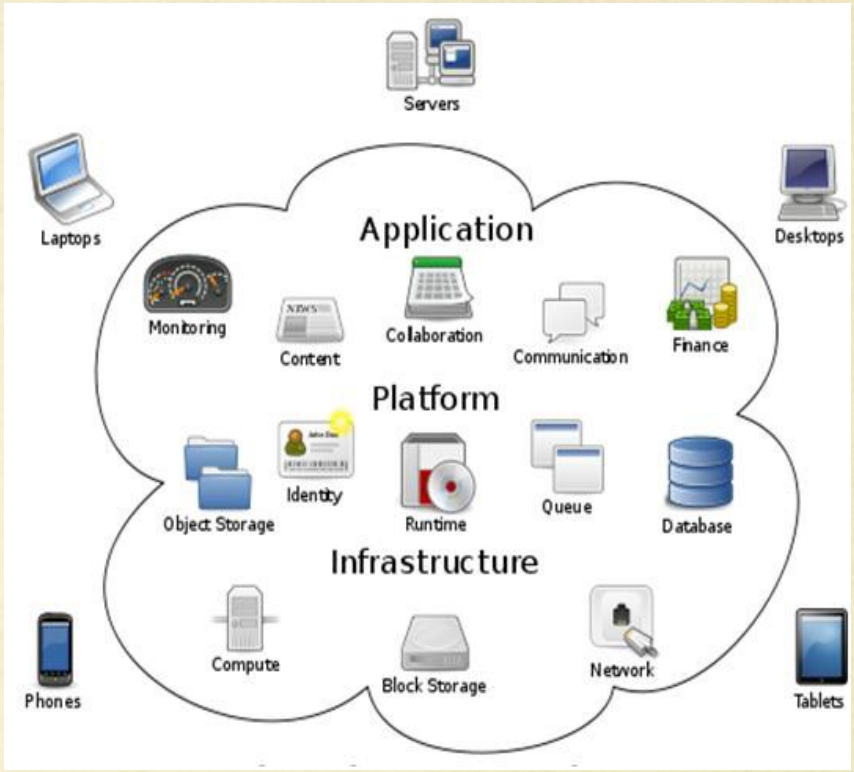
Evoluzione degli attacchi



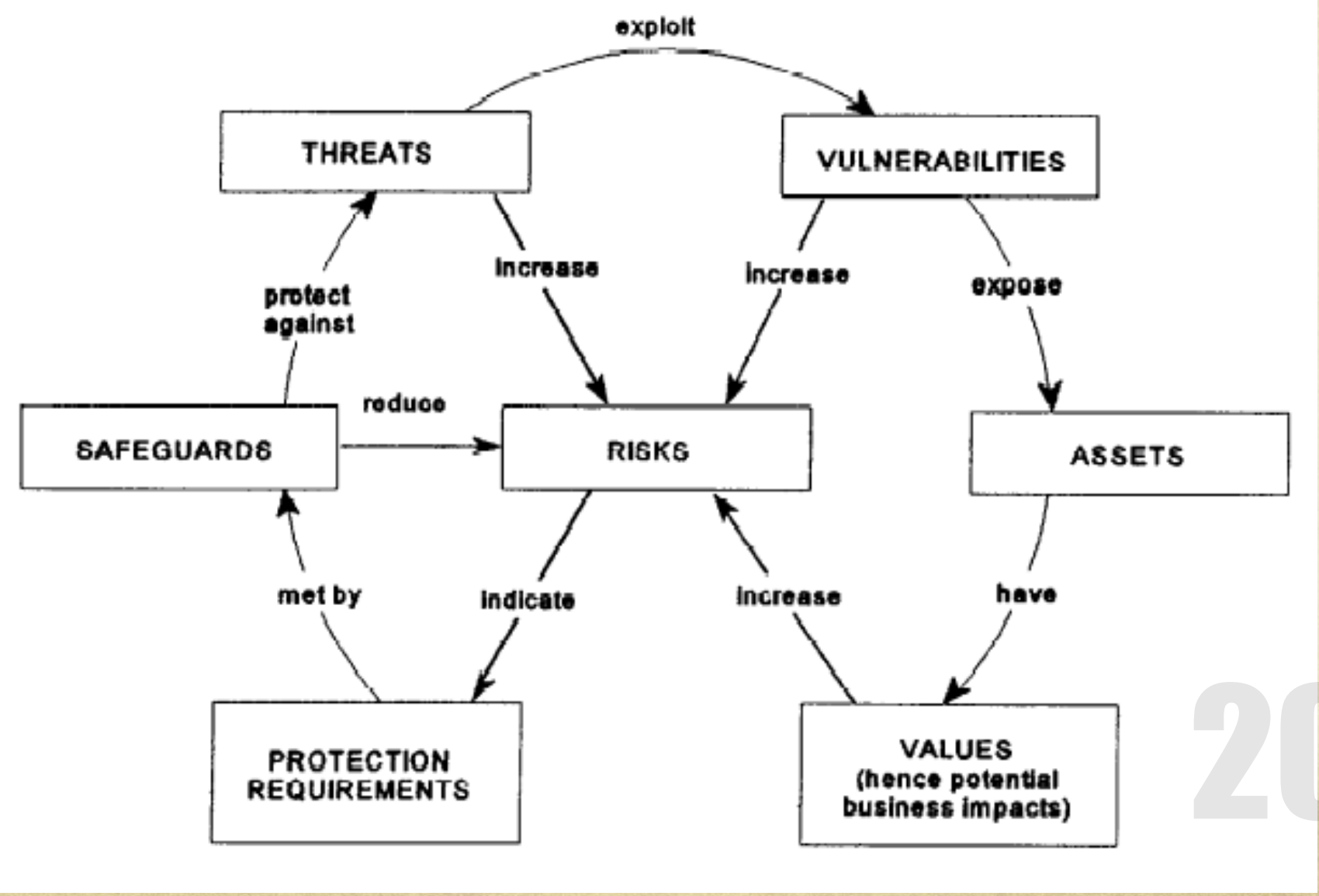
Cloud

Vantaggi del cloud

- **Abbassamento dei costi:** sottoscrivere software "in the cloud" riduce considerevolmente l'investimento
- **Costi di supporto inferiori:** Possibilità di avere versioni più aggiornate dei programmi, senza bisogno di supporto IT per l'aggiornamento
- **Rischi ridotti:** la sicurezza dei dati viene garantita dell'hosting provider
- **Accesso ai servizi in ogni momento e in ogni luogo:** Si lavora sui propri documenti via web, da casa o in qualsiasi altro luogo



Relazioni nella gestione del rischio



Sicurezza = Processo dinamico

- Evoluzione delle strategie di attacco
- Disponibilità di strumenti innovativi per contrastare gli attacchi
- Gestione Incidenti di sicurezza

Pensate un attimo...

- a cosa accadrebbe se Internet non funzionasse:
  - per un giorno
  - una settimana
  - un mese

- No eMail
- No BlackBerry
- No eCommerce

Tutti i servizi virtuali di business, contabili, commerciali, di pagamento e anche i sistemi di vendita si fermerebbero, e così tantissime aziende

I Social Network

- I Social Network (in italiano “rete sociale”) consistono in un qualsiasi gruppo di persone connesse tra loro su una stessa rete e che hanno in comune vari vincoli. Nel campo informatico vengono denominati Social quei siti che offrono all’utenza di condividere on-line delle notizie
- I più importanti sono Facebook, MySpace, Twitter, Netlog, ecc.

Velocità di propagazione

- La velocità di propagazione delle notizie in Internet è spaventosa
- La rete internet ha memoria, come il nostro cervello, e ogni notizia inserita resta permanentemente memorizzata, modificando le caratteristiche di interconnessione tra i vari nodi
- Un utente di una rete sociale (es.: facebook) con degli amici sparsi in giro per il mondo immette un'informazione personale (es.: una sua foto)

Velocità di propagazione

- Dopo 1.2 minuti 4,920 elaboratori (gli "amici degli amici") dispongono dell'informazione, che resta memorizzata anche nei loro PC

Elapsed time: 00:01:20 (hh:mm:ss)

Velocità di propagazione

- Dopo 2.4 minuti – 341,015 elaboratori dispongono dell'informazione che è ormai impossibile tenere sotto controllo, e soprattutto eliminare dalla rete

Elapsed time: 00:02:40 (hh:mm:ss)

Considerazioni sul fenomeno dei reati informatici negli ultimi anni

- Le osservazioni dei fenomeni accaduti negli ultimi anni hanno evidenziato un deciso cambiamento delle motivazioni e degli obiettivi che sono alla base della produzione e della diffusione dei virus informatici (malware) e più in generale dei codici realizzati al fine di arrecare danno

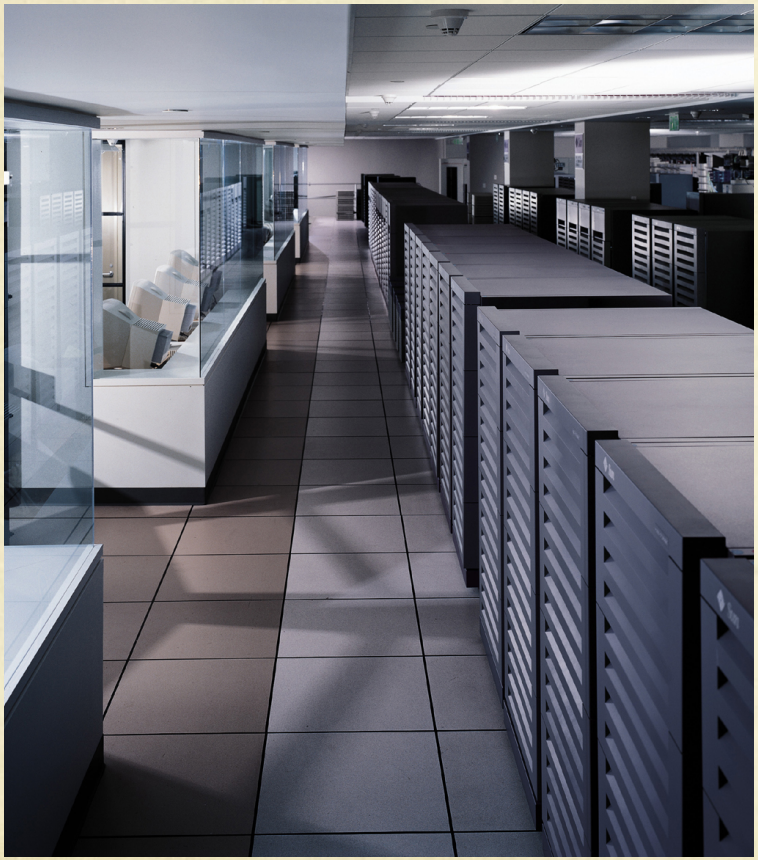
- E' sensibilmente diminuita la produzione di virus (I-Worm) di tipo tradizionale, mentre è aumentata quella di Spyware e Cavalli di Troia, anche se nel complesso i codici noti hanno superato l' impressionante numero di 200.000

- Le azioni criminose, a volte, sono addirittura organizzate su larga scala, attraverso la creazione di reti virtuali di computer dette "Botnet". Queste "reti" sono costituite da computer di utenti INCONSAPEVOLI i cui PC sono stati raggiunti da appositi software. L'attività è anche favorita dal fatto che la realizzazione di Trojan risulta più semplice e breve delle attività necessarie alla creazione di un virus o di un Worm

I pericoli maggiori per un'azienda sono rappresentati non tanto dagli attacchi provenienti dall'esterno, quanto piuttosto dai cosiddetti Insider

- Un dipendente di un'azienda può essere in possesso di conoscenze e di permessi tali da poter compromettere l'integrità dei dati aziendali, eventualmente in collaborazione con aggressori esterni, in quanto può fornire loro tutti gli strumenti per sfruttare eventuali vulnerabilità del sistema informatico o semplicemente divulgare dati sensibili, riservati o ad elevata criticità

Opportunità e motivazioni



- Un dipendente di una grande organizzazione può avere motivazioni psicologiche per utilizzare le conoscenze e i privilegi di accesso alle applicazioni e condurre quindi un attacco ai danni dell'azienda per la quale lavora o per la quale ha prestato servizio

- Gli attacchi portati a buon fine provenienti dall'esterno sono decisamente rari. Spesso i dati riservati sono resi noti da personale interno, ad esempio gli addetti ai CED, oppure dipendenti con profili aziendali ad alto livello di accesso ad applicazioni ed ambienti di elevata importanza e criticità

Considerazioni sul fenomeno dello Spam e dell'ingegneria sociale

- L'uso dello spam, per il quale non si registrano diminuzioni di tendenze, ha permesso di raffinare tecniche finalizzate ad ingannare gli utenti e sottrarre loro informazioni puntando sulla buona fede delle persone. Anche le grandi tragedie che la collettività mondiale ha subito negli scorsi anni sono state usate in tale ambito

- Ad esempio, le notizie inerenti l'uragano Katrina furono utilizzate come spunto per generare messaggi di Spam e Phishing, di cui almeno uno contenente un collegamento verso un sito che, sfruttando una nota vulnerabilità di IE, scaricava ed installava un Trojan nel PC

- Attualmente lo stesso fenomeno si sta riscontrando nei messaggi che invitano alla solidarietà verso la popolazione di Haiti colpita dal devastante terremoto

Considerazioni finali e alcune misure di sicurezza e prevenzione

- Paradossalmente l'utilizzo di questi strumenti, estremamente semplici ed immediati soprattutto per le nuove generazioni, allontanano sempre di più l'utente finale dalle conoscenze specifiche di ciò che avviene all'interno delle procedure informatiche (fatta ovviamente eccezione per programmatori, analisti, sistemisti, tecnici e così via)

Il grado di sicurezza maggiore per un sistema informatico è direttamente proporzionale alla preparazione, alla formazione personale e competenza tecnica della persona che lo utilizza

Assurance & Confidence

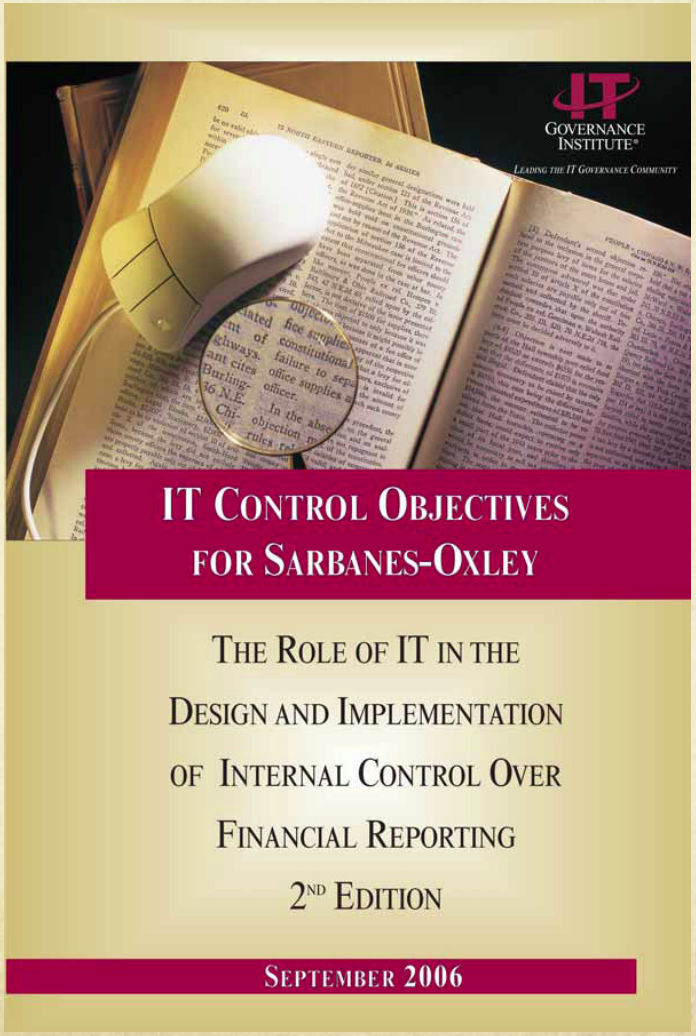
- US TCSEC fornisce una classificazione per le funzionalità di sicurezza (D, C1, C2, B1, B2, B3, A1)

- La normativa europea ITSEC fornisce una classificazione e valutazione dei prodotti e dei sistemi (E1..E6) e una valutazione delle funzionalità di sicurezza

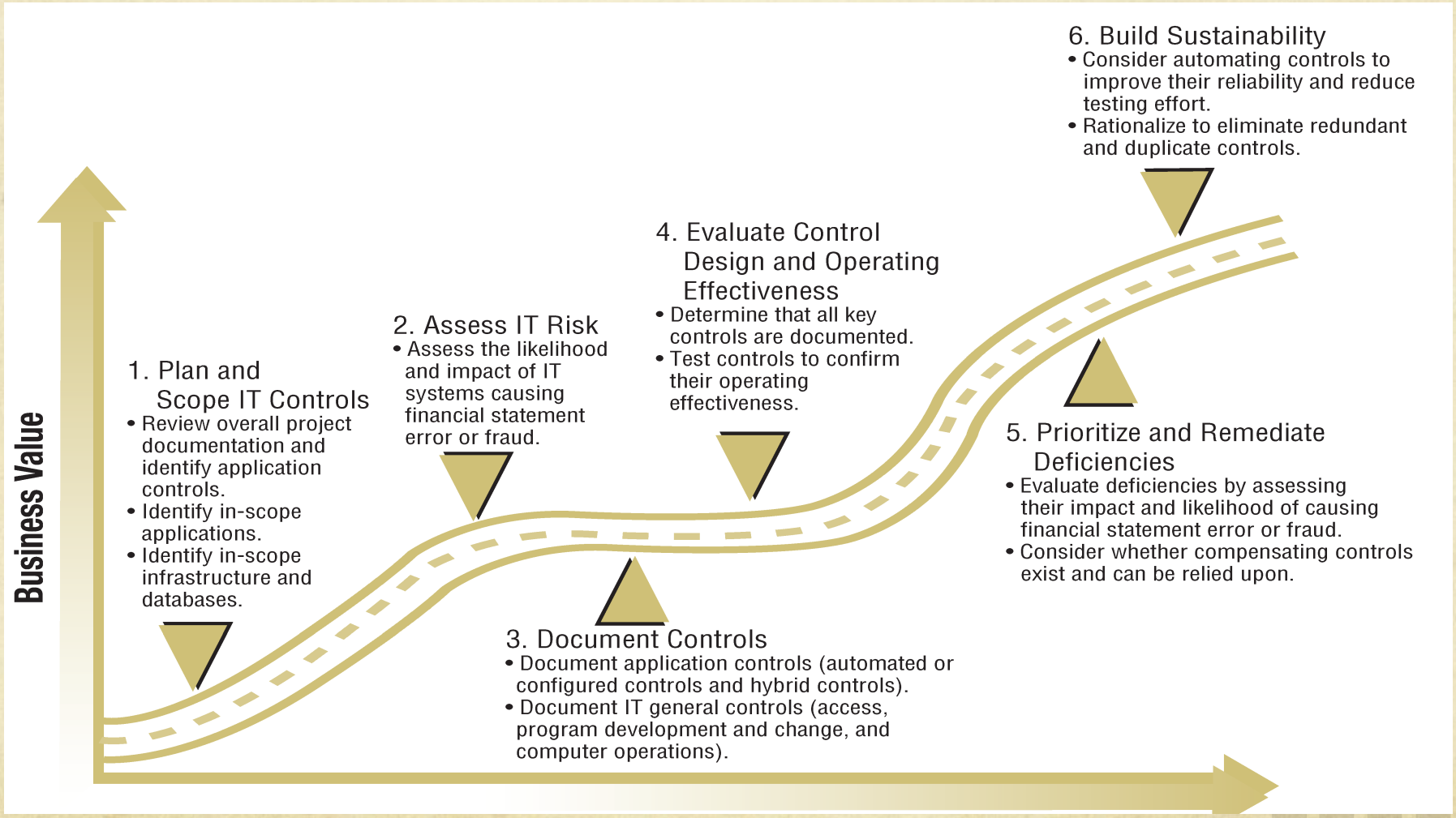
Governance, Risk and Control: CObIT5

ISACA®
Sistemi informativi: averne fiducia e trarne valore
Rome Chapter

Metodologia IT Governance Institute



Metodologia IT Governance Institute



Un parere autorevole

“

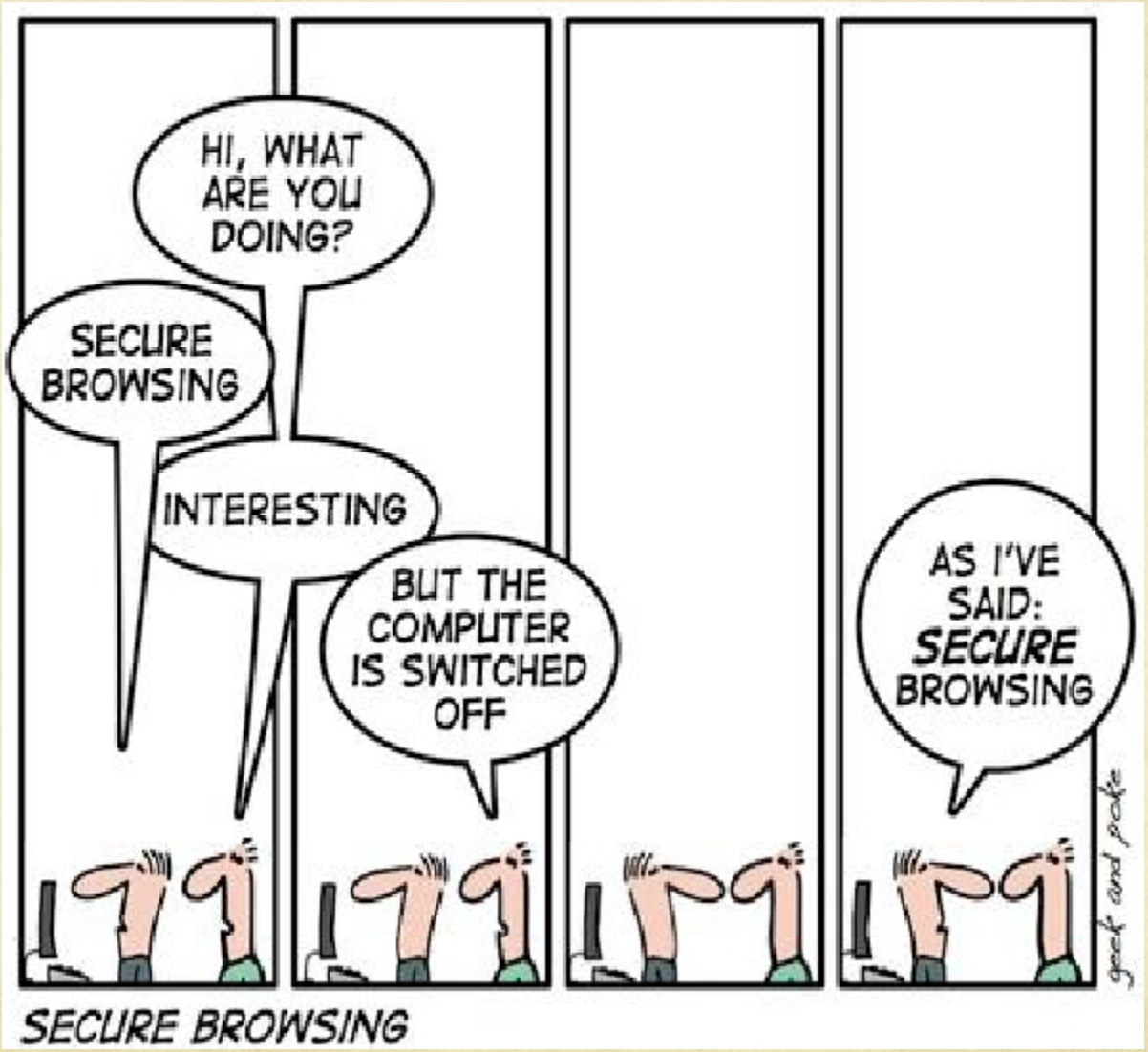
La sicurezza delle informazioni rimarrà una chimera finché esisterà il fattore umano

”

K. Mitnick

Come contrastare gli attacchi interni

Politiche di gestione del personale	Politiche di gestione coerenti alle responsabilità assegnate e ai ruoli occupati sono fondamentali per consentire al personale di svolgere in maniera “serena” il proprio compito in azienda
Alternanza dei compiti	Un frequente cambio di attività, pur nel rispetto delle professionalità dei singoli, riduce sensibilmente il rischio di messa in atto di attività illecite.
Separazione dei ruoli	Il criterio della separazione dei ruoli consente di mantenere un elevato controllo dei processi senza introdurre elementi esterni al processo stesso
Sistema dei controlli interni	La complessità delle aziende moderne può essere governata solo grazie alla presenza di un sistema ben definito di controlli che coinvolge principalmente i manager responsabili dei processi di business
Qualificazione e audit dei fornitori di servizi	Un processo di qualificazione dei fornitori è irrinunciabile per avere garanzie sul servizio ma un controllo formale sul campo ed eventuali approfondimenti del processo di qualificazione aiutano a migliorarne anche il livello di sicurezza



SECURE BROWSING

Grazie per l'attenzione!