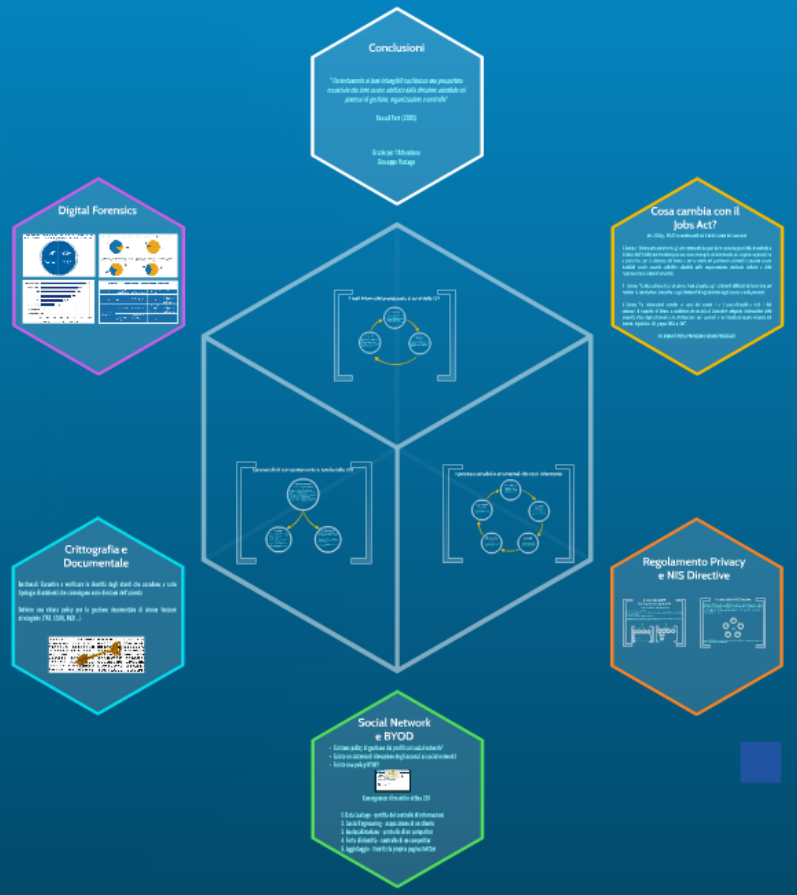
GDPR e Investigazioni Aziendali

Giuseppe Vaciago - Partner R&P Legal
twitter: https://twitter.com/giuseppevaciago
linkedin: http://it.linkedin.com/in/vaciago
email: giuseppe.vaciago@replegal.it

BRAINSTORM ELEMENTS

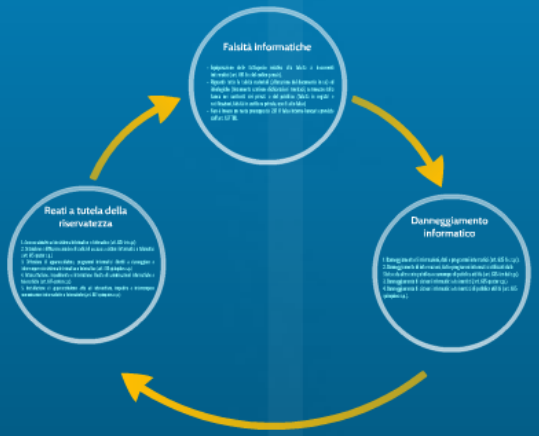


GDPR e Investigazioni Aziendali

Giuseppe Vaciago - Partner R&P Legal
twitter: https://twitter.com/giuseppevaciago
linkedin: http://it.linkedin.com/in/vaciago
email: giuseppe.vaciago@replegal.it

BRAINSTORM ELEMENTS

I reati informatici presupposto ai sensi della 231



Falsità informatiche

- Equiparazione delle fattispecie relativa alla falsità ai documenti informatici (art. 491-bis del codice penale).
- Riguarda tutte le falsità materiali (alterazione del documento in sè) ed ideologiche (documento contiene dichiarazioni mendaci) commesse dalla banca nei confronti dei privati o del pubblico (falsità in registri e notificazioni, falsità in scrittura privata, uso di atto falso)
- Non è invece un reato presupposto 231 il falso interno bancario previsto dall'art. 137 TUB.

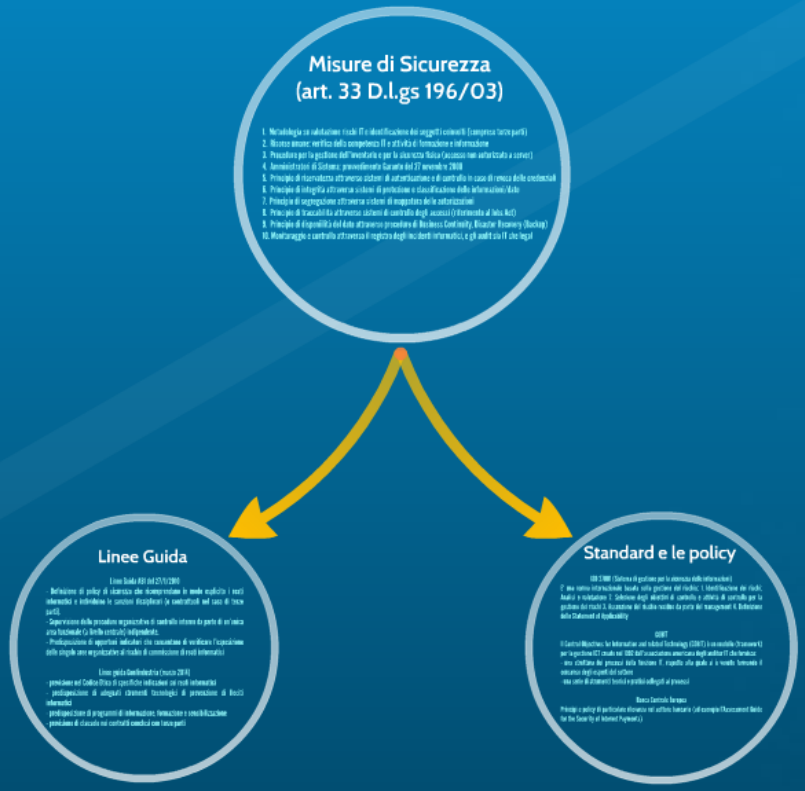
Danneggiamento informatico

1. Danneggiamento di informazioni, dati e programmi informatici (art. 635-bis c.p.).
2. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità (art. 635-ter del c.p.).
3. Danneggiamento di sistemi informatici o telematici (art. 635-quater c.p.).
4. Danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635-quinquies c.p.).

Reati a tutela della riservatezza

1. Accesso abusivo ad un sistema informatico o telematico (art. 615-ter c.p.)
2. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-quater c.p.)
3. Diffusione di apparecchiature, programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-quinquies c.p.)
4. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-quater c.p.)
5. Installazione di apparecchiature atte ad intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 617-quinquies c.p.)

I protocolli di comportamento a tutela della 231



Misure di Sicurezza (art. 33 D.l.gs 196/03)

1. Metodologia su valutazione rischi IT e identificazione dei soggetti coinvolti (comprese terze parti)
2. Risorse umane: verifica della competenza IT e attività di formazione e informazione
3. Procedure per la gestione dell'inventario e per la sicurezza fisica (accesso non autorizzato a server)
4. Amministratori di Sistema: provvedimento Garante del 27 novembre 2008
5. Principio di riservatezza attraverso sistemi di autenticazione e di controllo in caso di revoca delle credenziali
6. Principio di integrità attraverso sistemi di protezione e classificazione delle informazioni/dato
7. Principio di segregazione attraverso sistemi di mappatura delle autorizzazioni
8. Principio di traccabilità attraverso sistemi di controllo degli accessi (riferimento al Jobs Act)
9. Principio di disponiilità del dato attraverso procedure di Business Continuity, Disaster Recovery (Backup)
10. Monitoraggio e controllo attraverso il registro degli incidenti informatici, e gli audit sia IT che legal

Standard e le policy

ISO 27001 (Sistema di gestione per la sicurezza delle informazioni)

E' una norma internazionale basata sulla gestione del rischio: 1. Identificazione dei rischi; Analisi e valutazione 2. Selezione degli obiettivi di controllo e attività di controllo per la gestione dei rischi 3. Assunzione del rischio residuo da parte del management 4. Definizione dello Statement of Applicability

COBIT

Il Control Objectives for Information and related Technology (COBIT) è un modello (framework) per la gestione ICT creato nel 1992 dall'associazione americana degli auditor IT che fornisce:

- una struttura dei processi della funzione IT, rispetto alla quale si è venuto formando il consenso degli esperti del settore
- una serie di strumenti teorici e pratici collegati ai processi

Banca Centrale Europea

Principi e policy di particolare rilevanza nel settore bancario (ad esempio l'Assessment Guide for the Security of Internet Payments)

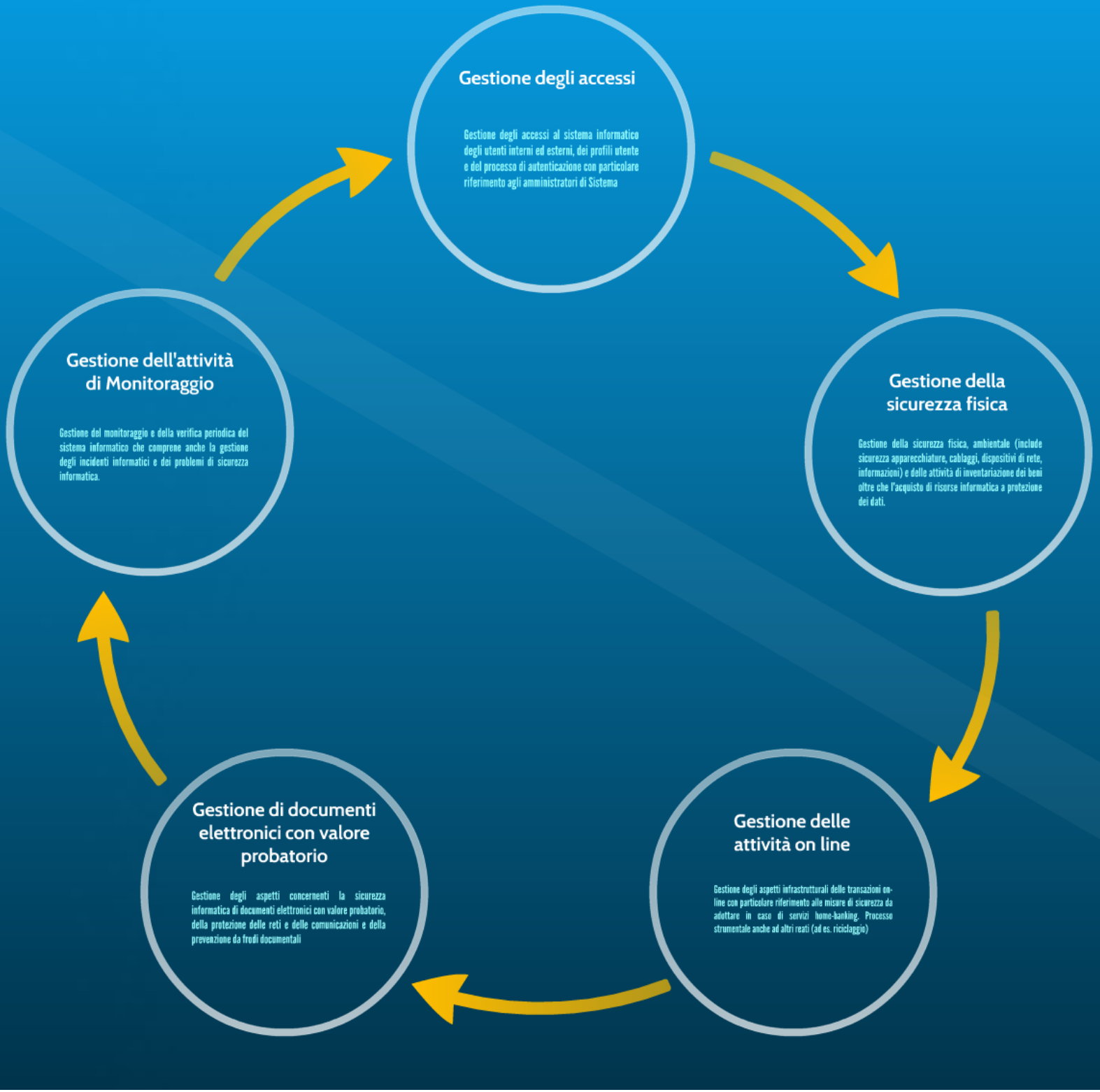
Linee Guida

Linee Guida ABI del 27/1/2010

- Definizione di policy di sicurezza che ricomprendano in modo esplicito i reati informatici e individuino le sanzioni disciplinari (o contrattuali nel caso di terze parti).
- Supervisione delle procedure organizzative di controllo interno da parte di un'unica area funzionale (a livello centrale) indipendente.
- Predisposizione di opportuni indicatori che consentano di verificare l'esposizione delle singole aree organizzative al rischio di commissione di reati informatici

Linee guida Confindustria (marzo 2014)

- previsione nel Codice Etico di specifiche indicazioni sui reati informatici
- predisposizione di adeguati strumenti tecnologici di prevenzione di Ileciti informatici
- predisposizione di programmi di informazione, formazione e sensibilizzazione
- previsione di clausole nei contratti conclusi con terze parti


Gestione degli accessi
Gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione con particolare riferimento agli amministratori di Sistema
Gestione della sicurezza fisica
Gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni) e delle attività di inventariazione dei beni oltre che l'acquisto di risorse informatica a protezione dei dati.
Gestione delle attività on line
Gestione degli aspetti infrastrutturali delle transazioni on-line con particolare riferimento alle misure di sicurezza da adottare in caso di servizi home-banking. Processo strumentale anche ad altri reati (ad es. riciclaggio)
Gestione di documenti elettronici con valore probatorio
Gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni e della prevenzione da frodi documentali
Gestione dell'attività di Monitoraggio
Gestione del monitoraggio e della verifica periodica del sistema informatico che comprene anche la gestione degli incidenti informatici e dei problemi di sicurezza informatica.

Gestione degli accessi

Gestione degli accessi al sistema informatico degli utenti interni ed esterni, dei profili utente e del processo di autenticazione con particolare riferimento agli amministratori di Sistema

Gestione della sicurezza fisica

Gestione della sicurezza fisica, ambientale (include sicurezza apparecchiature, cablaggi, dispositivi di rete, informazioni) e delle attività di inventariazione dei beni oltre che l'acquisto di risorse informatica a protezione dei dati.

Gestione delle attività on line

Gestione degli aspetti infrastrutturali delle transazioni on-line con particolare riferimento alle misure di sicurezza da adottare in caso di servizi home-banking. Processo strumentale anche ad altri reati (ad es. riciclaggio)

Gestione di documenti elettronici con valore probatorio

Gestione degli aspetti concernenti la sicurezza informatica di documenti elettronici con valore probatorio, della protezione delle reti e delle comunicazioni e della prevenzione da frodi documentali

Gestione dell'attività di Monitoraggio

Gestione del monitoraggio e della verifica periodica del sistema informatico che comprene anche la gestione degli incidenti informatici e dei problemi di sicurezza informatica.

Cosa cambia con il Jobs Act?

Art. 23 D.lgs. 151/15 in modifica dell'art. 4 dello Statuto dei Lavoratori

1. Comma: “Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell’attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e *per la tutela del patrimonio aziendale* e possono essere installati p*revio accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali.*

2. Comma: “La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore *per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.*”

3. Comma: "Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro *a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli* e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

E IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI?

Regolamento Privacy e NIS Directive

Il ruolo del GDPR
EU Regulation 2016/679

I requisiti in termini di sicurezza informatica sono i seguenti:

Il ruolo della NIS Directive

La Direttiva 2016/1148 chiamata anche NIS (Network and Information Security) è una normativa che fornisce un livello per i fornitori di servizi essenziali tra cui sono compresi anche i fornitori di servizi digitali. I settori coperti dalla NIS directive sono sostanzialmente quelli legati alle infrastrutture critiche: energia, trasporti, banche, finanza, salute e settore idrico. Se è vero che sono ricompresi anche i fornitori di servizi digitali non è ricompresa il settore della robotica e dei suoi produttori. Gli elementi fondanti della direttiva sono:

References: DIGITALEUROPE's, *Views on the Internet of Things*, Brussels, 14 April 2015 - goo.gl/UCo2Wz; Chris Jannes, *Cybersecurity Law and the Internet of Things*, 8 June 2016 - http://www.scl.org/site.aspx?i=ed47867

Il ruolo del GDPR
EU Regulation 2016/679

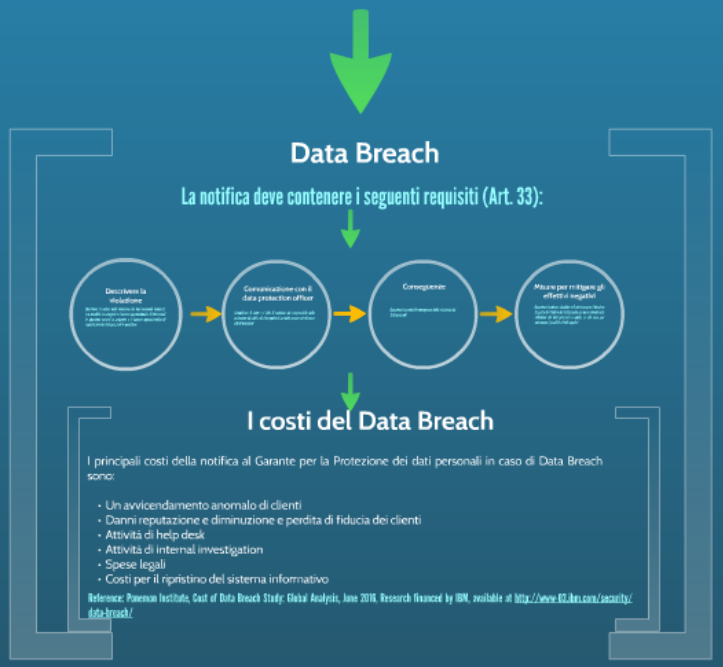
I requisiti in termini di sicurezza informatica sono i seguenti:

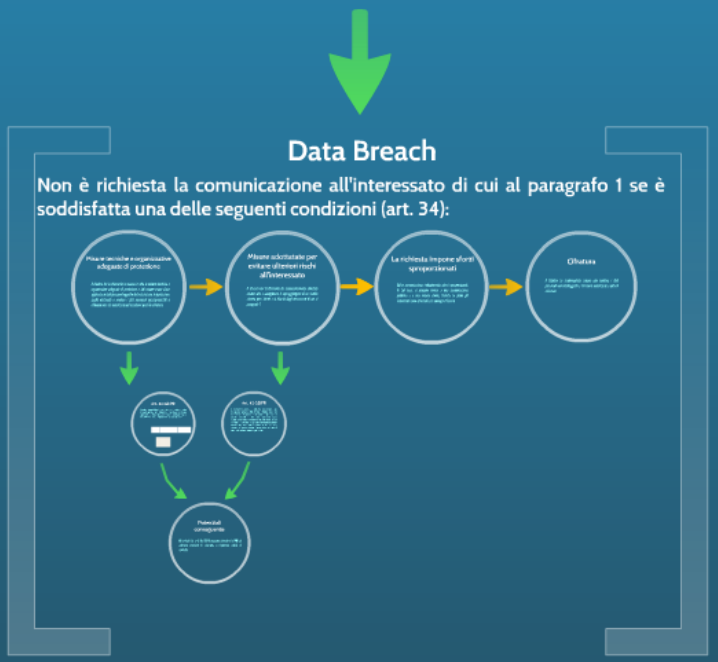
I principali requisiti di sicurezza imposti dal Regolamento Europeo sulla Privacy sono:

1. Un sistema deve poter garantire: (i) la pseudonimizzazione e la cifratura dei dati personali; (ii) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; (iii) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; (iv) Testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento (art. 32)

2. Ove possibile, una descrizione generale delle misure di sicurezza tecniche e organizzative di cui all'articolo 32 (art. 30)

3. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche





Data Breach

La notifica deve contenere i seguenti requisiti (Art. 33):

I costi del Data Breach

I principali costi della notifica al Garante per la Protezione dei dati personali in caso di Data Breach sono:

- Un avvicendamento anomalo di clienti
- Danni reputazione e diminuzione e perdita di fiducia dei clienti
- Attività di help desk
- Attività di internal investigation
- Spese legali
- Costi per il ripristino del sistema informativo

Reference: Ponemon Institute, Cost of Data Breach Study: Global Analysis, June 2016, Research financed by IBM, available at http://www-03.ibm.com/security/data-breach/

Descrivere la violazione

Descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione

Comunicazione con il data protection officer

Comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni

Conseguenze

Descrivere le probabili conseguenze della violazione dei dati personali

Misure per mitigare gli effettivi negativi

Descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi

I costi del Data Breach

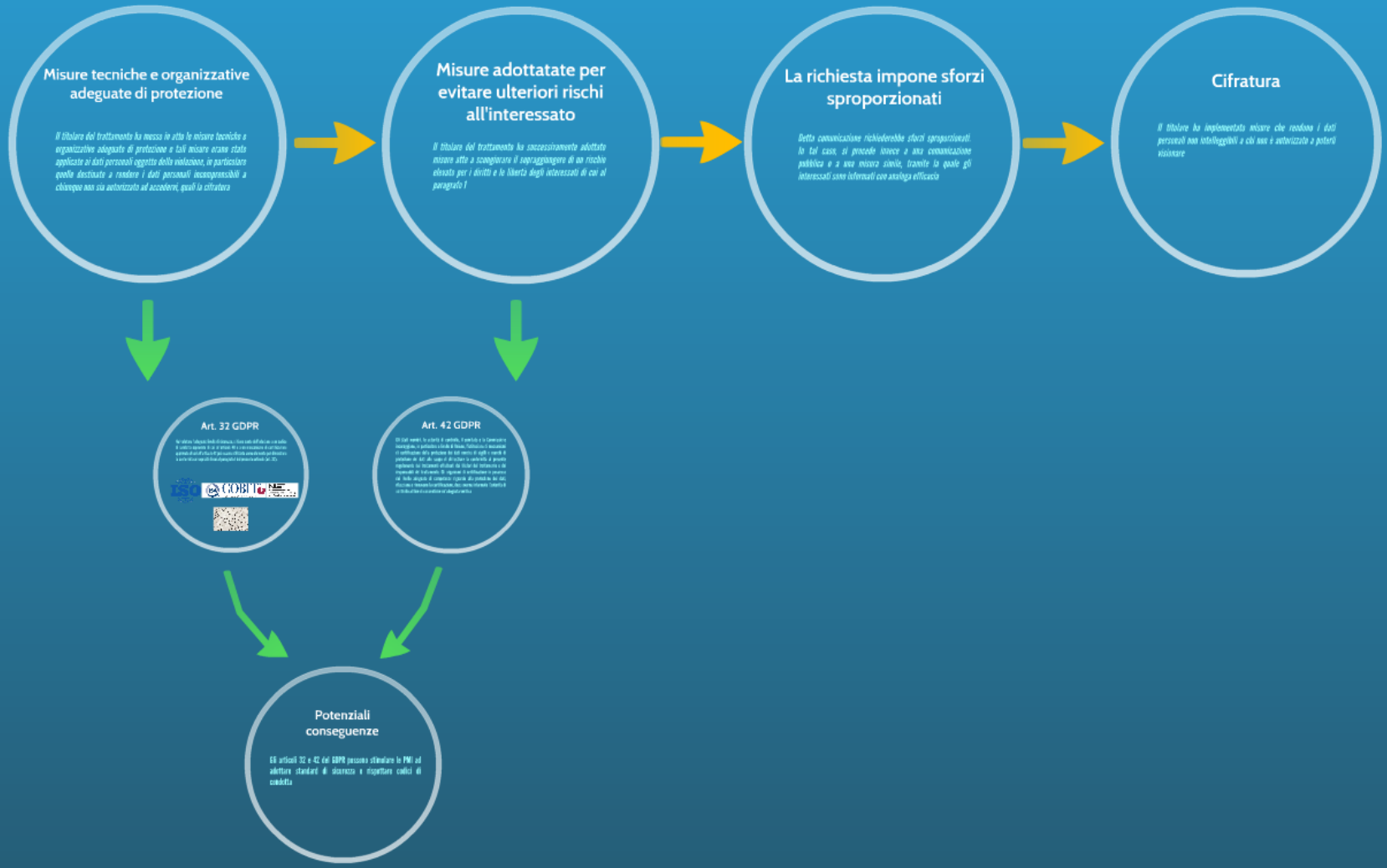
I principali costi della notifica al Garante per la Protezione dei dati personali in caso di Data Breach sono:

- Un avvicendamento anomalo di clienti
- Danni reputazione e diminuzione e perdita di fiducia dei clienti
- Attività di help desk
- Attività di internal investigation
- Spese legali
- Costi per il ripristino del sistema informativo

Reference: Ponemon Institute, Cost of Data Breach Study: Global Analysis, June 2016, Research financed by IBM, available at http://www-03.ibm.com/security/data-breach/

Data Breach

Non è richiesta la comunicazione all'interessato di cui al paragrafo 1 se è soddisfatta una delle seguenti condizioni (art. 34):



Misure tecniche e organizzative adeguate di protezione

Il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura

Misure adottatate per evitare ulteriori rischi all'interessato

Il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati di cui al paragrafo 1

Art. 32 GDPR

Nel valutare l'adeguato livello di sicurezza, si tiene conto dell'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo (art. 32).

Art. 42 GDPR

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentirne un'adeguata verifica

Potenziali conseguenze

Gli articoli 32 e 42 del GDPR possono stimolare le PMI ad adottare standard di sicurezza e rispettare codici di condotta

Art. 32 GDPR

Nel valutare l'adeguato livello di sicurezza, si tiene conto dell'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo (art. 32).

ISO

ISA COBIT 5
AN ISACA® FRAMEWORK

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Art. 42 GDPR

Gli Stati membri, le autorità di controllo, il comitato e la Commissione incoraggiano, in particolare a livello di Unione, l'istituzione di meccanismi di certificazione della protezione dei dati nonché di sigilli e marchi di protezione dei dati allo scopo di dimostrare la conformità al presente regolamento dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento. Gli organismi di certificazione in possesso del livello adeguato di competenze riguardo alla protezione dei dati, rilasciano e rinnovano la certificazione, dopo averne informato l'autorità di controllo al fine di consentirne un’adeguata verifica

Potenziali conseguenze

Gli articoli 32 e 42 del GDPR possono stimolare le PMI ad adottare standard di sicurezza e rispettare codici di condotta

La richiesta impone sforzi sproporzionati

Detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia

Cifratura

Il titolare ha implementato misure che rendono i dati personali non intelleggibili a chi non è autorizzato a poterli visionare

Il ruolo della NIS Directive

La Direttiva 2016/1149 chiamata anche NIS (Network and Information Security) è una normativa che fornisce un livello per i fornitori di servizi essenziali tra cui sono compresi anche i fornitori di servizi digitali. I settori coperti dalla NIS directive sono sostanzialmente quelli legati alle infrastrutture critiche: energia, trasporti, banche, finanza, salute e settore idrico. Se è vero che sono ricompresi anche i fornitori di servizi digitali non è ricompreso il settore della robotica e dei suoi produttori. Gli elementi fondanti della direttiva sono:

Reference: DIGITALEUROPE's, *Views on the Internet of Things*, Brussels, 14 April 2016 - goo.gl/UCsQWz; Chris James, *Cybersecurity Law and the Internet of Things*, 6 June 2016 - http://www.scl.org/site.aspx?i=ed47867


National Information Security Strategy
National Information Security Strategy: Obbligo per gli Stati Membri di adottare una strategia nazionale sulla sicurezza delle reti e dei sistemi informativi
Rete di Cooperazione
Realizzazione di un network europeo che si occupi della sicurezza delle reti critiche
CSIRTs Network
individuazione per ogni Stato Membro di un'autorità nazionale competente per la sicurezza delle informazioni e creare una squadra di "pronto intervento"
Data Breach
Vengono stabiliti degli obblighi di notifica in caso di data breach per le società e i fornitori di servizi digitali
Point of Contact
Vengono imposti degli obblighi per gli Stati Membri di creare dei punti di contatto per lo scambio di informazioni tra le autorità.
NIS Directive in a nutshell

Social Network e BYOD

- Esistono policy di gestione dei profili sui social network?
- Esiste un sistema di rilevazione degli accessi ai social network?
- Esiste una policy BYOD?

Conseguenze rilevanti in ottica 231

1. Data Leakage - perdita del controllo di informazioni
2. Social Engineering - acquisizione di un cliente
3. Geolocalizzazione - controllo di un competitor
4. Furto di identità - controllo di un competitor
5. Aggiotaggio - tramite la propria pagina twitter

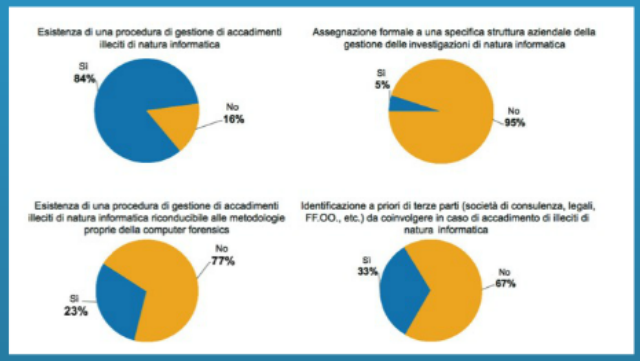
Crittografia e Documentale

Gestionali: Garantire e verificare le identità degli utenti che accedono a varie tipologie di ambienti che coinvolgono varie divisioni dell'azienda

Definire una chiara policy per la gestione documentale di alcune funzioni strategiche (TAX, LEGAL, R&D ...)

Digital Forensics

È necessario un sistema di gestione con un approccio di tipo preventivo rispetto alle esigenze di investigazione informatica, fondato su 4 presupposti:



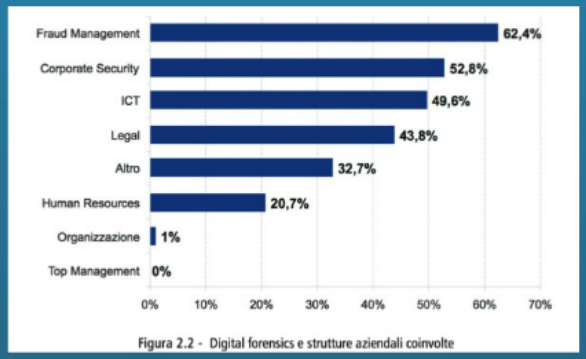


Figura 2.2 - Digital forensics e strutture aziendali coinvolte

Mappatura (asset inventory) delle fonti di prova digitale

Fonte di prova	Tempi di conservazione	Luogo e modalità di conservazione	Copie di back up	Note
CCTV	**72** ore	Registrazione su server dedicato	No	Tempi di conservazione compliant con Garante Privacy
Log di accesso applicazione X	**6** mesi log in e log out	Registrazione su log server "xyz"	Si – Copie notturne registrazione su nastro	Tempi di conservazione compliant con Garante Privacy
	1 mese log in utenti generici	Registrazione in locale su application server	No	

Mappatura (asset inventory) delle fonti di prova digitale

Fonte di prova	Tempi di conservazione	Luogo e modalità di conservazione	Copie di back up	Note
CCTV	**72** ore	Registrazione su server dedicato	No	Tempi di conservazione compliant con Garante Privacy
Log di accesso applicazione X	**6** mesi log in e log out	Registrazione su log server “xyz”	Si – Copie notturne registrazione su nastro	Tempi di conservazione compliant con Garante Privacy
	1 mese log in utenti generici	Registrazione in locale su application server	No	

Conclusioni

"l'orientamento ai beni intangibili costituisce una prospettiva essenziale che deve essere adottata dalla direzione aziendale nei processi di gestione, organizzazione e controllo"

Russel Parr (2005)

Grazie per l'Attenzione
Giuseppe Vaciago

GDPR e Investigazioni Aziendali

Giuseppe Vaciago - Partner R&P Legal
twitter: https://twitter.com/giuseppevaciago
linkedin: http://it.linkedin.com/in/vaciago
email: giuseppe.vaciago@replegal.it

BRAINSTORM ELEMENTS